

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application)

Applicant: Tokutani et al.)

Serial No.)

Filed: October 6, 2003)

For: PRIVATE DATA PROTECTION)
DISTRIBUTION METHOD)
AND PROGRAM)

Art Unit:)

I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Mail Stop PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date.

Oct. 6, 2003
Date

Daniel Canan
Express Mail Label No.: EV032735215US

CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

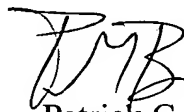
Japanese Patent Application No. 2002-296778, filed October 9, 2002

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By



Patrick G. Burns

Registration No. 29,367

October 6, 2003

300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Telephone: 312.360.0080
Facsimile: 312.360.9315

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: October 9, 2002

Application Number: Patent Application
No. 2002-296778
[ST.10/C]: [JP2002-296778]

Applicant(s): FUJITSU LIMITED

August 18, 2003

Commissioner,
Japan Patent Office Yasuo IMAI

Certificate No. P2003-3067294

1503.68508
312.360.0080

96

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 9 日
Date of Application:

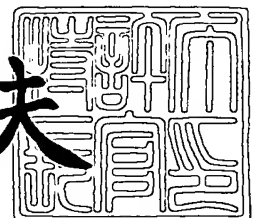
出 願 番 号 特 願 2 0 0 2 - 2 9 6 7 7 8
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 2 9 6 7 7 8]

出 願 人 富 士 通 株 式 会 社
Applicant(s):

2 0 0 3 年 8 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 3 - 3 0 6 7 2 9 4

【書類名】 特許願

【整理番号】 0251343

【提出日】 平成14年10月 9日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明の名称】 個人データ保護流通方法及びプログラム

【請求項の数】 5

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

 【氏名】 徳谷 崇

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

 【氏名】 畠山 卓久

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

 【氏名】 松永 宏

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100074099

 【住所又は居所】 東京都千代田区二番町 8 番地 2 0 二番町ビル 3 F

 【弁理士】

 【氏名又は名称】 大菅 義之

 【電話番号】 03-3238-0031

【選任した代理人】**【識別番号】** 100067987**【住所又は居所】** 神奈川県横浜市鶴見区北寺尾 7 - 2 5 - 2 8 - 5 0 3**【弁理士】****【氏名又は名称】** 久木元 彰**【電話番号】** 045-573-3683**【手数料の表示】****【予納台帳番号】** 012542**【納付金額】** 21,000円**【提出物件の目録】****【物件名】** 明細書 1**【物件名】** 図面 1**【物件名】** 要約書 1**【包括委任状番号】** 9705047**【プルーフの要否】** 要

【書類名】 明細書

【発明の名称】 個人データ保護流通方法及びプログラム

【特許請求の範囲】

【請求項 1】 暗号化された個人データを受信するステップと、
暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信するステップと、
前記復号鍵と個人データ使用ライセンスを復号するステップと、
前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断するステップと、
前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号するステップとを有することを特徴とする個人データ保護流通方法。

【請求項 2】 前記復号鍵と個人データ使用ライセンスは D R M 認証技術を用いて暗号化及び復号化されることを特徴とする請求項 1 に記載の個人データ保護流通方法。

【請求項 3】 前記個人データ使用ライセンスを D R M 認証技術を用いて復号化するための機構は、T R M 化されていることを特徴とする請求項 2 に記載の個人データ保護流通方法。

【請求項 4】 前記暗号化された個人データ及び該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを複数の情報主体より受信するステップと、

複数の前記個人データ使用ライセンスを同一な条件の単位で連結して名簿ライセンスを作成するステップと、

該名簿ライセンスの作成に使用された個人データ使用ライセンスに対応する、暗号化された個人データを連結して名簿を作成するステップを有することを特徴とする付記 1 に記載の個人データ保護流通方法。

【請求項 5】 暗号化された個人データを受信するステップと、
暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信するステップと、

前記復号鍵と個人データ使用ライセンスを復号するステップと、
前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断するステップと、
前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号するステップとをコンピュータに実行させることを特徴とする個人データ保護流通プログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

情報主体から個人情報を取得し、利用する個人情報取扱業者において、情報主体からその個人情報の使用を制限する個人データ保護流通システムに関する。

【 0 0 0 2 】

【従来の技術】

近年、プライバシーマーク制度、個人情報に関する様々な省庁から出されたガイドラインや個人情報保護法案また、W 3 Cで策定されている P 3 P など個人情報の取り扱いについて関心が集まっている。

【 0 0 0 3 】

W 3 C (World Wide Web Consortium) は、インターネット上で利用できるサービスの各種標準仕様を策定する目的で、1 9 9 4 年に米 M I T コンピュータ・サイエンス研究所 (Massachusetts Institute of Technology, Laboratory for Computer Science) に設立された非営利団体である。HTML や XML など、様々なインターネット標準を策定している。また、P 3 P (Platform for Privacy Preferences) は、Webサイトのプライバシー・ポリシーを記述するための標準フォーマットである。W 3 Cによって現在標準化が進められている。これにより、ユーザ側のエージェント・ソフトウェアが、当該Webサイトのプライバシー・ポリシーを自動的に取得して解釈し、あらかじめユーザによって設定された個人情報の取扱基準に照らし合わせて、その挙動を切り替えられるようになる。

【 0 0 0 4 】

例えば、Webサイトまで要求しないまでも、Cookieを使用して、サイトをアクセスしているユーザを特定し、ユーザの挙動をモニタしていたりするところが少なくない。従来、こうしてWebサイト側が入手した個人情報が、どのようなポリシーに沿って運用されるかを確認するには、各サイトのプライバシー・ポリシーをユーザ自身が調査する必要があった。こうした処理をソフトウェアが自動的に行えるように、サイトのプライバシー・ポリシーを標準的なフォーマットで記述するために考案されたものがP 3 Pである。これにより、ユーザは、あらかじめWebブラウザなどで個人情報の取扱基準を設定しておき、Webサイトのプライバシー・ポリシーがこの基準に逸脱しないかどうかを自動的に判断できるようになる。

【0005】

このように、P 3 Pは、アクセスしたWebサイトのプライバシー・ポリシーをソフトウェアが自動的に取得、解釈するための技術的なメカニズムを提供するが、記述されたポリシー通りにWebサイトが運営されるかどうかを保証するものではないので注意が必要である。また、P 3 P自体には、ユーザとWebサイトの間で個人情報を安全に転送する手段は規定されていない。データを安全に転送するためには、別の手段を講じる必要がある。

【0006】

特に、米Harris Interactive社の意識調査によると、個人情報に関する一般消費者の関心事の内、消費者の懸念事項のトップには「企業が無断で個人情報を他の企業と共有すること」が挙げられており、また企業が信頼に値するかを判断する上で重要視するトップ項目には、「顧客の個人情報を当人の許可無く、あるいは法律によって求められない限り開示しない」という事項が挙げられている。

【0007】

したがって、個人が、安心して個人情報を提供するには、最低限個人情報の運用に関して二次使用の禁止や目的外使用の禁止、また、個人が自分の個人情報がどこでどのように使用されているかの把握と制御（情報主体のコントロール権）が重要であると考えられる。

【0008】

また、各省庁のガイドラインや日本工業規格の J I S Q 15001、あるいは（2002年4月）現在法律案ではあるが、個人情報保護法案などの様々なガイドラインや認定評価制度、法律においても上記3点に加え、事業者の個人情報の安全管理、及び安全な収集について重要視している。

【0009】

以上をまとめると、個人データを保護するためには、少なくとも以下の5つの要件を満足しなければならない。

（1）事業者は、情報主体に対して個人データの使用目的を告知し、その目的範囲内で使用しなければならない。（目的外の使用・不正使用の禁止）

（2）事業者は、不正に個人データを提供してはならない。（不正提供・二次使用の禁止）

（3）事業者は、個人データを安全に保管し、管理しなければならない。（安全な保管・管理）

（4）事業者は、個人データを安全に収集しなくてはならない。（安全な収集）

（5）事業者は、情報主体に対して、要求があった場合には、いつでもその情報主体の個人データを開示したり、訂正したり、削除しなければならない。（情報主体のコントロール権の確保）

従来では次のような対策を講じている。

（1）企業内で個人情報管理規定を定め、遵守する。

（2）（1）と同様、企業内で個人情報管理規定を定め、遵守する。たとえば、特定の従業員にしか個人データが保管しているデータベースへのアクセス権を与えないといったものがある。

（3）以下のような対策が採られている。

【0010】

（ア）外部からアクセスできない場所におく。

（イ）個人データを暗号化などして保存する。

（ウ）パスワード認証によりアクセスしてくる個人の正当性を判断し、その後ロールベース（役職などに基づいて）のアクセス制御によりどのファイルにアクセスできるかを制御する。

【0011】

(エ) だれが、どのようなアクセスをしたのかのログを記録する。

(オ) データのバックアップ。バックアップしたメディアなどをロッカーなどに鍵をかけて保管する。

(4) 予め情報主体に同意を得た上で提供してもらう。そのとき、個人データは、暗号通信などを使って送られる。

(5) サイト上でアカウントを取得し、サイト上で自分の個人データを確認、訂正、削除などをできるようにする。

【0012】

また、現在行われている個人情報を取り扱うサービスにおいて、センターが個人ユーザから個人データを収集し、それを運用するセンタ集中管理が存在する。このようなサービスでの個人データの運用には、例えば、個人ユーザから興味ある分野の情報を収集していると、その分野の企業と契約し、代理広告をするといったものがある。従来のこのような集中管理の形態では、センタが個人情報を管理して、個人データは、センタから第三者に提供をするといったことはなかった。

【0013】

また、個人情報ではないが、著作権保護に関し、最近では、DRM (Digital Rights Management) という技術が使用されている。DRMとは、利用許可条件とその条件に従って動作する機構からなっている。利用許可条件には、例えば、利用回数や利用期限、コピー回数などがある。(下記、非特許文献1、2 参照)

従来の電子データのプライバシーに関する取り組みとしては、ユーザが、Cookieなどのデジタル・オブジェクトや実行ファイルについて受け入れるか拒否することを指定可能とする技術がある(特許文献1 参照)。また、個人情報管理センタが個人情報提供者と個人情報利用者との仲立ちを行う構成を有する技術がある(特許文献2 参照)。

【0014】**【特許文献1】**

特表平 1 0 - 5 1 2 0 7 4 号公報（米国特許 6, 3 6 3, 4 8 8 号明細書）

【 0 0 1 5 】

【特許文献 2】

特開 2 0 0 1 - 2 6 5 7 7 1 号公報

【 0 0 1 6 】

【非特許文献 1】

穴澤健明、武村浩司、常広隆司、長谷部高行、畠山卓久：コンテンツ保護の柔軟化を実現した開放型超流通基盤、情報処理学会 電子化知的財産・社会基盤研究会報告、2 0 0 1 年 1 1 月<online><http://www.keitaide-music.org/pdf/EIP14-5.pdf>

【 0 0 1 7 】

【非特許文献 2】

畠山卓久、丸山秀史、千葉哲央：音楽コンテンツの超流通とセキュリティ、F U J I T S U, Vol.52, No.5, p.473-481, 2001年9月. <http://magazine.fujitsu.com/>

【 0 0 1 8 】

【発明が解決しようとする課題】

1) 個人情報保護に関して上記従来技術で挙げた(2)及び(3)の(ウ)の対策では、正当なアクセス権を持っているものが、勝手に情報をコピーしたり、改ざんしたり、削除したりするといった不正な使用が可能である。

2) 上記従来技術で挙げた(1)に対して、目的範囲内での使用は、正当なアクセス権を持っているものに対して個人情報規定などといった行動規範による対策しか行われておらず、実質的に目的外使用に関しては、情報処理技術による対策は存在しない。

3) 従来技術で挙げた要件(5)に対する解決策は、センタだけが個人データを保有し、管理するといった形態の解決方法である。したがって、センタが個人データを第三者に提供した後、個人データが点在するような環境において開示・訂正・削除といった対策は存在しない。

4) 上記センタ集中管理による個人情報取り扱いに関するサービスでは、センタ

から一旦個人データを事業者に提供してしまうと、提供された事業者は、他の事業者へ不正に販売するなど、現在のところセンタから第三者へ個人データを提供するという事はしない。

【0019】

本発明の課題は、情報主体の制御の下、個人情報の流通を情報主体の意思に従って制御することができる個人情報保護流通システムを提供することである。

【0020】

【課題を解決するための手段】

本発明の個人データ保護流通方法は、暗号化された個人データを受信するステップと、暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信するステップと、前記復号鍵と個人データ使用ライセンスを復号するステップと、前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断するステップと、前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号するステップとを有することを特徴とする。

【0021】

したがって、本発明によれば、個人データの取得者の個人データの使用方法を、個人データの提供者（情報主体）が、自ら個人データ使用ライセンスを作成することによって、制限することができる。したがって、個人データの提供者の制御の下に、提供者の個人データが流通することになるので、個人データの提供者は、自分の個人データが思わぬところで不正に使用されることを防止することができる。

【0022】

【発明の実施の形態】

本発明の実施形態においては、以下のような構成を採用する。

1) 不正な使用の禁止に関しては、TRM (Tamper Resistant Module) 化したDRM (Digital Rights Management) でしか利用できないようにすることにより、改ざんや削除が禁止される。このとき、更に使用ライセンスの使用条件

に T R M 化した D R M 装置を移動する毎に移動回数が 1 ずつ減るような移動可能回数を設け、かつ、使用ライセンスに、コピー可能条件を設けないかあるいは、設けても 0 と設定することにより、不正コピーが禁止される。

2) 目的外使用に関しては、使用ライセンスの使用目的という条件により解決される。具体的には、個人データを利用するアプリケーションを使用目的別に分類し、各アプリケーションの使用目的が識別できる状態にしておき、個人データを使用するときに、その使用ライセンスの使用条件に対応するアプリケーションでしか利用できないような D R M 機構を備えておく。

3) 情報主体からの個人データの情報主体への開示請求においては、センタ（事業者の一種であるが、個人データの管理を主な業務としている事業者である）への開示請求によって実現できる。そして、センタが個人データを提供した他の事業者に関しては、センタが作成した個人データをどの事業者に提供したかのリストを情報主体に提供することにより、その情報主体の個人データを保有している全ての事業者に対して、情報主体が開示請求を行うことを可能にする。

【0023】

個人データの訂正請求に関しては、情報主体は、センタに個人データの訂正要求を出し、訂正の後の個人データの訂正情報が各事業者間で同期され解決される（ここで、同期とは、各事業者間で同じ個人データを有するように、各事業者に対し個人データの更新を行うことを示す）。

【0024】

個人データの削除請求に関しては、情報主体は、個人データを記載した名簿リストから削除してもらいたい事業者を特定し、その事業者の名簿リストから自分の個人データを直接削除してもらうことにより解決される。あるいは、センタに個人データの削除要求を出し、センタにある名簿リストから削除してもらう。このとき、センタの名簿リストが削除されたことにより、センタから名簿リストの提供を受けた事業者の保有する名簿リストに対しても、同様の削除が行われる。

4) 上記 3 つの手段をセンタ及びセンタが個人データを提供する事業者に適用し、情報主体には、クライアントコンピュータを設置することにより安全な個人データの流通が可能になる。このとき、ライセンスの価格を設定するなどしてビジ

ネスとして商業ベースにのせることもできる。なお、センタが事業者に個人データを提供するときは、名簿リスト単位で事業者を提供する。

1. 概要

1. 1 問題提起

図1は、情報主体、事業者、第三者の関係を説明する図である。

【0025】

情報主体、事業者、第三者の3者からなる構成を考える。情報主体、事業者、第三者は、それぞれ、ネットワークで接続されたコンピュータを有している。事業者は、そのコンピュータの個人情報データベースに情報主体の個人データを持っている。第三者は、情報主体の個人データを取得したい要求がある。

【0026】

そこでまず、情報主体と事業者との間において以下のことが満足していなくてはならない。

[事業者の情報主体に対する要件]

(1) 事業者は、情報主体に対して個人データの使用目的を告知し、その目的範囲内で使用しなければならない。(目的外使用・不正使用の禁止)

(2) 事業者は、不正に個人データを提供してはならない。(不正提供・二次使用の禁止)

(3) 事業者は、個人データを安全に保管しなくてはならない。(安全な保管)

(4) 事業者は、個人データを安全に収集しなければならない。(安全な収集)

(5) 事業者は、情報主体に対して、要求があった場合には、いつでもその情報主体の個人データを開示したり、訂正したり、削除しなければならない。(情報主体のコントロール権の確保)

これら4つの要件を満足した上で、事業者は、第三者に個人データを提供する。このときも、第三者は、事業者に対して、少なくとも上記要件と同様なことが満足されなければならない。すなわち、

[第三者の事業者に対する要件]

(6) 第三者は、情報主体に対して個人データの使用目的を告知し、その目的範囲内で使用しなければならない。(目的外使用・不正使用の禁止)

(7) 第三者は、不正に個人データを提供してはならない。(不正提供・二次使用の禁止)

(8) 第三者は、個人データを安全に保管しなければならない。(安全な保管)

(9) 第三者は、個人データを安全に収集しなくてはならない。(安全な収集)

(10) 第三者は、情報主体に対して、要求があった場合にはいつでもその情報主体の個人データを開示したり、訂正したり、削除しなければならない。(情報主体のコントロール権の確保)

である。

【0027】

本発明の実施形態では、これら10個の要件を満足する実現法を提案する。

1. 2 解決方法の概要

1. 1 節の問題に対する解決法として以下のようにする。

【0028】

図2は、本発明の実施形態の構成の概略構成を説明する図である。

基本的には、個人データの使用にDRM技術を利用する。すなわち、個人データを暗号化し、その暗号化個人データの使用ライセンスを発行し(ライセンスを発行できるのは、情報主体のみ)、個人データを利用するときには、DRM機能をもつアプリケーションでしか利用できないようにする。このようにすることで、まず、個人データの不正使用(二次使用・目的外使用)が制御できる。

【0029】

また、事業者たちが使用ライセンスを保管し、利用する装置をTRM化することにより、個人データの安全な保管が実現され、更にライセンスを送受するとき暗号通信をすることにより個人データの安全な収集が可能である。

【0030】

そして、事業者たちは開示、訂正、削除といったサービスを情報主体に提供することで、情報主体のコントロール権を確保する。

すなわち、

情報主体

・ 個人データを暗号化する

- ・ 個人データの使用条件である使用ライセンスを発行する。
- ・ ライセンスを暗号通信で送信する。

事業者、第三者

- ・ ライセンスを送受するときは暗号通信を用いる。
- ・ ライセンスは、T R M化されたD R M認証機能を有するユニットに保管する。
- ・ D R M認証機能を持つ適切なアプリケーションで個人データを使用する。
- ・ 情報主体による個人データの開示・訂正・削除請求に応じる。

2. 情報主体－事業者間での個人データの保護

サービス事業者（個人データの管理を主に行う事業者ではなく、個人データの利用を目的とする事業者）が情報主体へ個人情報提供の提供を要求する場合、一般的には以下のようなやりとりが行われる。

（1）個人情報提供要求

- ・ サービス業者から情報主体へ個人情報提供を要求する。
- ・ このとき、サービス業者は、情報主体へ「サービス業者の名称」、「問い合わせ先」、「提供してもらう個人情報の項目」、「利用目的」などの情報を通知する。
- ・ また、提供した場合どのようなサービスが受けられるかなどの情報も通知する。

（2）個人情報提供の意思決定

- ・ 情報主体は、サービス業者から受け取った情報から、個人情報提供をしようかどうかを判断する。

（3）個人情報提供

- ・ 提供する場合、情報主体は、自分の個人データを作成し、サービス業者へ提供する。

（4）個人情報を利用する

- ・ サービス業者は、受け取った個人情報を情報主体に提示した利用目的の範囲内で利用する。

【0031】

以上が一般的な個人情報提供の手続きであるが、本発明の実施形態では（3）

と（４）を以下に示すような仕組みを用いることにより、遠隔から個人情報の不正な使用・目的外使用の制御を実現する。

２．１．個人情報の提供と個人情報利用の仕組み

図３は、情報主体が個人情報を提供することに同意した場合の提供の仕組みと、サービス業者がその情報を利用する仕組みを示す図である。

【００３２】

個人データ１０は、情報主体の持つコンピュータのクライアントツール２０が生成した共通鍵暗号方式の鍵１１を使って暗号化され、その暗号化個人データは、サービス業者のコンピュータ２１の個人データ・データベースシステム２２にネットワーク２５を介して送られ、アプリケーション２４が個人データを利用するときに、アプリケーション１０にロードされ、復号される。

【００３３】

個人データ使用ライセンス１２には、個人データ１０を暗号化するのに使用した共通鍵暗号方式の暗号鍵１１が入り、サービス業者のコンピュータ２１に設けられるライセンスデータベースシステム２３に、ネットワーク２５を介して送信される。このとき、個人データ使用ライセンス１２は、ライセンスデータベースシステム２３の公開鍵暗号方式の公開鍵１４と、ＤＲＭ認証に使用されるセッション鍵１３とで、二重に暗号化されて、ライセンスデータベースシステム２３に送信される。

２．１．１．情報主体による個人情報の編集

更に、図３を参照して説明を続ける。

【００３４】

情報主体２０は、個人データ１０を編集し、その個人データ１０に対して公開鍵暗号方式で暗号化する。暗号化は、住所、電話番号といった個人情報の各項目に対して鍵を生成し暗号化する。そして、個人データ使用ライセンス１２を作成する。このとき、個人データ使用ライセンス１２に、個人情報を暗号化したときの鍵１１が含まれる。これらの処理は、情報主体のクライアントツール２０により実行される。クライアントツールの機能としては、以下のものがある。

- ・ 使用ライセンスを発行する機能

- ・ 共通鍵暗号方式により個人データ 10 を暗号化・復号化する機能
- ・ 暗号鍵 13 を生成する機能
- ・ 暗号化個人データを受け渡す機能
- ・ 個人データ使用ライセンス 12 を送信する機能（DRM 認証ができる機能）

[個人データ使用ライセンス]

個人データ使用ライセンス 12 とは、個人データ 10 の使用条件を表現したものであり、個人データ 10 を利用する側は、この条件にしたがって実行される機構を持つアプリケーション 24 で使用する。

【0035】

個人データ使用ライセンス 12 には、暗号化個人データ 10 を復号するための復号鍵 11 と、その復号鍵で復号される暗号化個人データ 10 の識別子、そして使用条件から構成される。使用条件は、具体的には、以下のようなものがある。ただし、使用条件にはコピー回数は含めず、ライセンスをコピーすることはできないようにする。

- ・ 使用回数

情報主体 20 は、自分の個人データ 10 を利用する回数を制限できる。

- ・ 使用期限

情報主体 20 は、使用期限を指定できる。使用期限が過ぎたら、個人データ 10 の利用者側のライセンスデータベースシステム 23 から個人データ使用ライセンス 12 が強制的に削除される。

【0036】

情報主体 20 が個人データ 10 提供した相手に対して個人データ 10 の使用有効期限を決定することができる。

- ・ 移動回数

個人データ使用ライセンス 12 の、DRM 認証機能のついた装置間の移動回数を制限する。DRM 認証をする度毎に、サービス業者のコンピュータ 21 に移動回数を計数するために設けられたカウンタの値が 1 ずつ減る。

- ・ 使用目的

少なくとも、以下の使用目的属性を設ける。

ー調査と開発

個人データ 10 は、製品調査や、開発など、統計をとるようなアプリケーション 24 で実行される。

ー貸与・販売

ーデータマイニング

データマイニングするツールで実行される。

- ・提供許可業者

ライセンスを提供してもよい業種を記する。

- ・提供拒否サービス

どのようなサービスを受けたくないかを記述する。

- ・印刷回数

個人データ 10 を印刷して良い回数を記述する。

【0037】

図 4 は、使用条件と個人データの使用との関係を説明する図である。

上記した使用条件は、図 4 のように、個人データ使用ライセンスを提供するとき、及び個人データを使用するときに、参照され、個人データを使用する状況と使用条件のマッチングを行うことにより、ライセンスの提供・個人データの使用を制限する。

【0038】

すなわち、クライアントツールあるいは、第 1 のサービス業者から、第 2 のサービス業者に個人データが送信される場合には、個人データ使用ライセンスの使用条件である（1）提供許可業者にあたるか、（2）提供拒否サービスにあたるか、について判断し、提供可能な場合のみ個人データ使用ライセンスを提供する。また、第 2 のサービス業者のコンピュータのライセンスデータベースシステムから、第 2 のサービス業者のコンピュータ内のアプリケーションに個人データを移動する場合には、個人データ使用ライセンスの使用条件の移動回数を参照し、指定された回数以内で、個人データを移動できるか否かを判断し、個人データを移動するか否かを判断する。また、アプリケーションでは、個人データを使用する場合、個人データ使用ライセンスの（1）使用目的、（2）使用回数、（3）

使用期限などの条件を満たして、個人データを使用できるか否かを判断し、個人データを使用するか否かを決定する。

2. 1. 2 情報主体からの個人情報の提供

図3において、情報主体20は、暗号化された個人データ10と個人データ使用ライセンス12を作成した後、暗号化個人データをサービス業者21が保持している個人データ・データベースシステム22へ送り、個人データ使用ライセンス12をライセンスデータベースシステム23へ送る。個人データ・データベースシステム22及びライセンスデータベースシステム23へは、サービス業者21の従業員でも、特定のアクセス権を持つ者しかアクセスできない。個人データ使用ライセンス12を保存する装置は、すべてTRM化されているとする。

【0039】

個人データ使用ライセンス12の提供に関しては、DRM認証を用いる。

実際の利用場面において、サービス業者21は、利用期限・回数がなくなったときに、情報主体20に個人データ使用ライセンス12の継続使用についての要求を出し、情報主体20は、それに対して、受理・拒否の応答することを想定している。したがって、情報主体20がサービス業者21に個人データ10を提供する際、情報主体20は、利便性を考慮して、適当な使用期限や使用回数を設定した個人データ使用ライセンス12をサービス業者21に提供する。

2. 1. 3. サービス業者による個人情報の利用

サービス業者21は、個人データ提供要求のときに示した利用目的に合致したとき、TRM化された装置のDRM機能を持ったアプリケーション24でのみ個人データ10を利用できる。すなわち、図3において、暗号化された個人データ10は、個人データ・データベースシステム22からアプリケーション24に渡されるが、同時にライセンスデータベースシステム23に格納されている個人データ使用ライセンス12が秘密鍵15によって暗号化され、アプリケーション24に渡される。アプリケーション24では、暗号化された個人データ使用ライセンス12をDRM認証し、アプリケーション24において、個人データ使用ライセンス12を解読し、個人データ10の復号鍵11を取り出して、個人データ10をこの復号鍵11で復号して使用する。なお、このアプリケーション24は、

目的ラベルを持っており、その値が個人データ使用ライセンス 12 の目的属性と合致しない場合、その個人データ 10 を使用できないようになっている。ここで、アプリケーション 24 が持つ目的ラベルとは、個人データ使用ライセンス 12 の使用目的属性を値域に持つ変数であり、アプリケーション作成メーカが、予めそのアプリケーション 24 に設定する、あるいは、プラグインなどで、この値が設定されることを想定する。

【0040】

図5は、DRM認証を説明する図である。

DRM認証は、図5に示すように、セッション鍵2（秘密鍵）を共有するためのプロトコルである。

【0041】

以下のDRM認証の説明においては、サービス業者のコンピュータと情報主体のクライアントツールとの間でDRM認証が行われるものとして説明する。まず、サービス業者のコンピュータから個人データの取得要求とサービス業者の証明書がクライアントツールに送られる（①）。次に、クライアントツールは、送られてきたサービス業者の証明書の検証を行い（②）、セッション鍵1を生成する（③）。そして、クライアントツールは、セッション鍵1をサービス業者のコンピュータに送り（④）、サービス業者のコンピュータは、セッション鍵2を生成する（⑤）。そして、セッション鍵1で暗号化して、セッション鍵2をクライアントツールに送信する（⑥）。

【0042】

ここで、④では、セッション鍵1をサービス業者の証明書にある公開鍵で暗号化し、送信する。⑥では、セッション鍵2は、セッション鍵1により共通鍵暗号方式により暗号化して送信される。

【0043】

図6は、クライアントツールの個人データ使用ライセンスの送信時のフローチャートである。

まず、ステップS10において、個人データ要求の受信が行われる。ステップS11では、個人データを提供するか否かを決定する。個人データを提供しない

場合には、ステップS 12において、エラー処理を行い、処理を終了する。ステップS 11において、個人データを提供すると決定された場合には、ステップ13に進み、個人データを作成する。そして、ステップS 14において、共通鍵暗号方式の鍵を生成し、ステップS 15において、個人データを暗号化する。そして、ステップS 16において、個人データ使用ライセンスを生成し、ステップS 17において、暗号化個人データを送信する。ステップS 17においては、暗号化された個人データをDRM認証し、DRM認証が無効の場合には、ステップS 19において、エラー処理を行い、処理を終了する。ステップS 18のDRM認証において、認証結果が有効と判断された場合には、ステップS 20において、個人データ使用ライセンスを送信して、処理を終了する。

【0044】

図7は、個人データと個人データ使用ライセンスとの関係を説明する図である。

個人データを使用する際には、暗号化個人データの他に、個人データ使用ライセンスが用いられ、個人データ使用ライセンスの使用目的に「データマイニング」が設定されていた場合、個人データを使用するサービス業者側のアプリケーションでは、その目的ラベルに「データマイニング」が設定されていないと、使用できない仕組みとなっている。

【0045】

図8は、サービス業者のコンピュータのアプリケーションで個人データを使用する際のフローチャートである。

まず、ステップS 30において、アプリケーションは、暗号化個人データをロードする。ステップS 31では、ライセンスデータベースシステムから対応する個人データ使用ライセンスを受信し、個人データ使用ライセンスが有効か否かを判断する。ステップS 31において、無効と判断された場合には、ステップS 32において、アプリケーションは、個人データの使用拒否通知を受信し、処理を終了する。このとき、ライセンスの移動回数は増やされない。

【0046】

ステップS 31において、有効と判断された場合には、ステップS 33におい

て、個人データ使用ライセンスの移動可能通知を受信する。すなわち、今回の移動が許容される移動回数内の移動であることを確認する。そして、ステップ S 34 において、個人データ使用ライセンスの DRM 認証を行う。この認証が無効となった場合には、ステップ S 35 において、エラー処理をする。ステップ S 34 において、DRM 認証の結果が有効となった場合には、個人データ使用ライセンスをステップ S 36 において、受信し、ステップ S 37 において、アプリケーションの使用目的と個人データ使用ライセンスの使用目的が一致するか否かを判断する。ステップ S 37 において、一致しないと判断された場合には、ステップ S 38 において、個人データ使用ライセンスをライセンスデータベースシステムに戻して、処理を終了する。

【0047】

ステップ S 37 において、一致すると判断された場合には、ステップ S 39 において、個人データ使用ライセンスの使用回数と使用期限が有効か否かを判断する。ステップ S 39 において、無効と判断された場合には、ステップ S 40 において、個人データ使用ライセンスをライセンスデータベースシステムに戻して、処理を終了する。ステップ S 39 において、有効と判断された場合には、ステップ S 41 において、個人データの復号を行い、個人データ使用ライセンスの使用可能回数を 1 回分差し引く。そして、ステップ S 42 において、個人データを使用し、ステップ S 43 において、個人データの使用が完了すると処理を終了する。

【0048】

図 9 は、ライセンスデータベースシステムのライセンス送信時のフローチャートである。

まず、ステップ S 50 において、アプリケーションから個人データ使用ライセンスの取得要求を受信する。ステップ S 51 において、要求された個人データ使用ライセンスは、移動可能か否かを判断する。ステップ S 51 において、移動が不可能と判断された場合には、ステップ S 52 において、アプリケーションへ個人データ使用ライセンスの移動拒否通知を行い、処理を終了する。ステップ S 51 において、移動が可能とされた場合には、ステップ S 53 において、移動可能

通知をアプリケーションに送信する。そして、ステップ S 5 4 において、個人データ使用ライセンスの D R M 認証を行う。ステップ S 5 4 の認証の結果、無効となった場合には、エラー処理をステップ S 5 5 において行い、処理を終了する。ステップ S 5 4 において、D R M 認証の結果、有効と判断された場合には、ステップ S 5 6 において、個人データ使用ライセンスをアプリケーションに送信（移動）して、処理を終了する。

【 0 0 4 9 】

図 1 0 は、本発明の実施形態の別の構成における適用例を説明する図である。

図 1 0 においては、情報主体 2 0 からサービス業者 1（センタのコンピュータ）が個人データと個人データ使用ライセンスを受け取り、保管して、他のサービス業者 2 のコンピュータ 2 1 a から個人データの使用要求を受け付け、個人データをサービス業者 2 に提供する構成を示している。なお、図 3 と同じ構成要素には同じ参照番号を付している。

【 0 0 5 0 】

サービス業者 2 のコンピュータ 2 1 がサービス業者 2 のコンピュータ 2 1 a から個人データの取得要求を受け取ると、暗号化された個人データをサービス業者 2 のコンピュータ 2 1 a の個人データ・データベースシステム 2 2 a に送ると共に、個人データ使用ライセンスを D R M 認証のためのセッション鍵と公開鍵方式の暗号鍵で暗号化して、ライセンスデータベースシステム 2 3 a に送信する。暗号化された個人データと個人データ使用ライセンスを受け取ったサービス業者 2 のコンピュータ 2 1 a における個人データの使用は、図 3 において説明したものと同様であるので、説明を省略する。

【 0 0 5 1 】

このように、本発明の実施形態においては、サービス業者 1 のように、個人データの管理を主に行い、他のサービス業者からの個人データの取得要求に応じて、個人データ使用ライセンスとともに、個人データを提供する構成が可能である。この場合、サービス業者 1 は、個人データ管理センタとなるものである。

2. 2. 開示請求

個人データ 1 0 を扱っているサービス業者 2 1 は、個人データ 1 0 を提供して

いる情報主体 20 から開示請求（個人データ 10 を情報主体 20 に提示すること）があった場合、情報主体 20 に対して個人データ 10 を開示しなければならない。図 11 は、情報主体から開示請求があった場合の開示の仕組みを示す図である。

①個人データ開示要求

- ・ 情報主体は、サービス業者へ自分の個人データの開示を要求する。

②暗号化個人データ+サービス業者作成データの送信

- ・ サービス業者は個人データ・データベースシステムから暗号化された状態の個人データとその情報主体に関する関連したサービス業者が作成したデータを情報主体にむけて送信する。例えば、サービス業者作成データには、サービス業者が銀行である場合、口座の残高情報などがある。
- ・ なお、サービス業者作成データは、その情報の内容により、暗号化される場合もある。

③復号

- ・ 情報主体は、以前に自分の個人データを暗号化した鍵で復号し、情報を見る。

2. 3. 訂正請求

個人データを扱っているサービス業者は、個人データを提供している情報主体から当該個人データの訂正請求があった場合、本人の要求かどうかを確認し、情報主体が要求するないように訂正しなければならない。

【0052】

図 12 は、情報主体からの個人データの訂正請求における動作を説明する図である。

①個人データ訂正要求

- ・ 情報主体は、サービス業者へ自分の個人データの訂正を要求する。

②暗号化

- ・ 情報主体は、自分の個人データを訂正したものを用意し、新たに暗号化鍵を生成し、訂正した個人データを暗号化する。

③暗号化個人データの送信

- ・ 情報主体は、暗号化した個人データをサービス業者に向けて送信する。

- ・サービス業者は、訂正前の暗号化個人データを削除し、新しいデータに更新する。

④個人情報使用ライセンスの提供

- ・情報主体は、暗号化鍵の情報が更新された個人データ使用ライセンスをサービス業者に提供する。
- ・サービス業者は、訂正前のライセンスを削除し、新しいものに更新する。

【0053】

図13は、サービス業者側の個人データの訂正処理のフローチャートである。

まず、ステップS60において、訂正要求を情報主体から受信する。ステップS61において、ユーザ認証を行い、訂正要求をしてきた情報主体であるユーザは、登録者か否かを判断する。ステップS61において、ユーザが登録者でないと判断された場合には、ステップS62において、エラー処理を行い、ステップS63において、訂正要求をしてきた者へ要求拒否通知を送信して、処理を終了する。

【0054】

ステップS61において、ユーザが登録者であると確認された場合には、ステップS64において、情報主体であるユーザに訂正データを要求する。そして、ステップS65において、訂正された暗号化個人データを受信し、ステップS66において、暗号化個人データの更新を行う。ステップS67において、個人データ使用ライセンスのDRM認証を行い、認証の結果が無効の場合には、エラー処理（ステップS68）、要求者への要求拒否通知の送信（ステップS69）を行って、処理を終了する。ステップS67において、DRM認証の結果が有効である場合には、ステップS70では、個人データ使用ライセンスを受信し、個人データ使用ライセンスを更新し（ステップS71）、ステップS72において、要求者へ訂正完了通知を送信して、処理を終了する。

2. 4. 削除請求

基本的には、2. 3節の訂正要求と同じことをする。異なる点は、訂正要求では、訂正した暗号化個人データと訂正した個人データ使用ライセンスを使って、以前に使用していたものを削除してから更新したが、削除請求の場合は、この更

新処理がいらないというところである。すなわち、単に、サービス事業者の有する暗号化個人データと個人データ使用ライセンスを削除するだけである。

【 0 0 5 5 】

情報主体が削除命令を強制する方法として以下が挙げられる。

[情報主体と個人データを取り扱うサービス業者との契約による削除]

情報主体は、例えば、ライセンスの使用条件を期間で限定する、あるいは、使用回数で制限する。こうすることにより、それを使っている個人データ取り扱いサービス業者は、使用回数や使用期間などの更新のために、情報主体に問い合わせに来る。そのときに、情報主体は、使用の継続を許可するかどうかを決定する。もし情報主体が、継続の許可をしなければ、個人データ取り扱いサービス業者は、その情報主体の個人データを使用することができなくなり、事実上、削除したことと同じになる。

[ライセンス代理提供サーバによる削除]

図 1 4 は、ライセンス代理提供サーバによる個人データの削除処理を説明する図である。

【 0 0 5 6 】

情報主体は、信頼できるライセンス代理提供サーバに暗号化個人データ、個人データ使用ライセンスを発行し、このサーバがサービス業者の要求に対して、情報主体の同意を得た上で、個人データ使用ライセンスを提供する。このサーバは、常時接続の状態にある。したがって、サービス業者は、いつでもサーバにアクセスして、個人データを要求することができる。個人データ使用ライセンスは、短い期間、例えば、1 日単位などでその使用条件を制限すれば、サービス業者は、個人データ使用ライセンスを更新するため、毎日ライセンス代理提供サーバにライセンスを要求してくることになる。したがって、情報主体がサービス業者に削除を請求する場合、情報主体は、ライセンス代理提供サーバに削除請求し、ライセンス代理提供サーバは、以後サービス業者にライセンスを発行しないことにより、情報主体の削除請求を実現する。

【 0 0 5 7 】

すなわち、以下のような処理の流れとなる。

①情報主体がクライアントツールを使って、ライセンス代理提供サーバに削除請求をする。

②サービス業者は、個人データを使用するために、個人データ使用ライセンスをライセンス代理提供サーバに要求する。

③しかし、ライセンス代理提供サーバは、情報主体から削除請求を受け取っているため、サービス業者に対して、個人データ使用ライセンスを発行しない。これにより、サービス業者は、当該情報主体の個人データを使用できなくなる。

2. 5. 個人情報をも単位で使用する

サービス業者は、大量の個人データを保持しているため、実際には、一人一人個別に個人データを使用するというよりも、ある単位でまとめた個人データを名簿として扱い、これを利用する。ここでは、このような名簿を使用するための仕組みについて説明する。

2. 5. 1. 名簿の作成と名簿ライセンスの生成

名簿は、個人データ使用ライセンスに含まれる使用条件の内、同一の使用条件となっている暗号化個人データを連結して、個人データ名簿として名簿データベースの中で保存される。これは、ライセンスデータベースに入っている個人データ使用ライセンスが更新される度に、個人データ使用ライセンスの内、同一の使用条件を有するものを集めて、整頓する。一つの同一使用条件の個人データ使用ライセンスのリストを名簿ライセンスと呼ぶ。この名簿ライセンスにある個人データを識別するIDに基づいて、暗号化個人データが表1のように、個人データ名簿となる。

【0058】

【表1】

ID	氏名	性別	生年月日	メールアドレス	電話番号	職業	・・・	興味ある分野
0001	〇〇〇	男	〇年〇月〇日	〇〇@〇〇〇	〇〇〇-〇〇〇	エンジニア	・・・	スポーツ
0002	△△△	男	△年△月△日	△△@△△△	△△△-△△△	教員	・・・	サイエンス
・	・	・	・	・	・	・	・	・
・	・	・	・	・	・	・	・	・
1111	×××	女	×年×月×日	××@×××	×××-×××	学生	・・・	旅行

【0059】

なお、ここで、個人データ名簿のID以外の項目は暗号化される。

また、名簿ライセンスについては、図15のように生成する。

図15は、名簿ライセンスの生成処理を説明する図である。

【0060】

各同一使用条件の個人データ使用ライセンスを組にし、それらに含まれる暗号化鍵を連結する。連結した鍵を使用条件と一緒にし、名簿ライセンスを生成する。このとき、名簿ライセンスそのものを識別し、かつ名簿ライセンスから名簿が参照できるよう識別子であるライセンサー名簿IDが付与される。

【0061】

生成された名簿ライセンスは、名簿ライセンスデータベースシステムに保存される。したがって、名簿ライセンスデータベースは、表2のようなエンティティのリストが保存されている。

【0062】

【表2】

ライセンサー名簿ID		XXX
条件	使用回数	100
	使用期限	2003年3月31日
	移動回数	100
	使用目的	マイニング
	提供可能業者	メーカー
	提供拒否サービス	ダイレクトメール
ライセンスID+鍵		X1 101000101
		X2 1100001111
		⋮ ⋮
		⋮ ⋮
		X1000 010101011
名簿ライセンスの鍵 (連結された鍵)		101000101 1100001111 ⋯ 010101011

【0063】

これらの処理は、名簿作成ツールが行う。ライセンスデータベースと名簿ライセンスデータベースは、物理的には同じデータベースシステム上にあってもよい。

。

【0064】

図16は、名簿の作成と名簿ライセンスの生成処理を図示した模式図である。

サービス業者は、複数の情報主体のコンピュータから、暗号化された個人データを収集し、個人データ・データベースに格納する。また、サービス業者は、各情報主体のコンピュータから個人データ使用ライセンスを受信し、ライセンスデータベースに格納する。名簿作成ツールは、ライセンスデータベースを参照し、同じ使用条件を持っている個人データを個人データ・データベースから探しだし、名簿にして名簿データベースに格納する。また、各個人データ使用ライセンスは、名簿作成ツールが、上記のようにして、名簿ライセンスにして、名簿ライセンスデータベースに格納する。なお、ここで、名簿作成ツール、ライセンスデータベース、及び名簿ライセンスデータベースはTRM化されたDRM機能を有する装置である。

【0065】

図17は、名簿作成ツールが名簿・名簿ライセンスを作成する処理のフローチャートである。

まず、ステップS80において、全ての個人データ使用ライセンスをロードする。次に、ステップS81において、個人データ使用ライセンスを使用条件別にソートする。ステップS82においては、同一使用条件の個人データ使用ライセンスを連結し、名簿ライセンスを作成する。ステップS83では、名簿ライセンスの個人データIDを取得し、ステップS84において、個人データIDから暗号化名簿の作成を、個人データ・データベースに要求する。そして、ステップS85において、名簿ライセンスを名簿ライセンスデータベースに保存して、処理を終了する。

2. 5. 2. 名簿の使用

名簿の使用も基本的には、2. 1. 3節と同じくTRM化された装置のDRM認証機能を持ったアプリケーション内でしか使用できない。

【0066】

図18は、名簿の使用形態を説明する図である。

サービス業者は、名簿データベースからアプリケーションに名簿をロードするが、同時に、DRM認証機能を使って、名簿ライセンスデータベースに補間されている名簿ライセンスをアプリケーションに渡す。そして、アプリケーションは、名簿ライセンスに従って、名簿を復号化して使用する。

2. 6. 名簿を使用する場合の開示請求

サービス業者が、名簿を使用する場合、情報主体からの開示請求に対してサービス業者は、個人情報データベースシステムに保存されている暗号化個人データとその情報主体の付加情報を合わせて送信する。従って、開示に関しては、2. 2 節と同様な方法となる。

2. 7 名簿を使用する場合の訂正請求

名簿を使用する場合の個人情報を訂正するには、サービス業者は、個人データデータベースシステムの古い個人データを削除し、訂正して個人データを受け取る。その後、名簿データベースシステムの関係する名簿の情報主体の項目を削除し、訂正した内容に変更する。個人データ使用ライセンスについても同様に、ライセンスデータベースシステムの古い個人データ使用ライセンスを削除し、訂正した個人データ使用ライセンスに変更する。その後、名簿ライセンスデータベースシステムの関係する名簿ライセンスの鍵を変更する。ただし、ライセンスに関しての変更点は、個人データを変更した項目における鍵であり、使用条件については変更しない。したがって、名簿ライセンスの変更箇所は、鍵のみとなる。

【0067】

図19は、名簿使用時の訂正要求の処理を説明する図である。

- ①クライアントツールからサービス業者に個人データの訂正要求が送信される。
- ②訂正した暗号化個人データを送信する。
- ③サービス業者の個人情報データベースにおいて、個人データを訂正する。
- ④次に、名簿データベースの名簿を訂正する。
- ⑤クライアントツールから訂正した個人データ使用ライセンスをサービス業者に送信する。
- ⑥ライセンスデータベースにおいて、個人データ使用ライセンスを訂正する。
- ⑦名簿ライセンスデータベースの名簿ライセンスを訂正する。

⑧サービス業者からクライアントツールに訂正完了通知が通知される。

【0068】

図20は、名簿使用時のサービス業者の名簿の訂正処理を示すフローチャートである。

まず、ステップS89において、訂正要求を受信する。ステップS90において、訂正要求をしてきた、情報主体である要求者は登録者であるか否かを判断する。ステップS90の判断がNOの場合には、エラー処理をステップS91において行い、ステップS92において、要求者へ要求拒否通知を送信する。

【0069】

ステップS90の判断がYESの場合には、ステップS93において、訂正データを要求者に要求する。ステップS94において、訂正された暗号化データを受信し、ステップS95において、個人データ・データベースを更新し、ステップS96において、名簿データベースを更新する。

【0070】

ステップS97においては、個人データ使用ライセンスの送受信のためのDRM認証を行う。ステップS97の結果が無効である場合には、ステップS98において、エラー処理を行い、ステップS99において、要求者へ要求拒否通知を送信する。ステップS97の結果が有効である場合には、ステップS100において、個人データ使用ライセンスを要求者から受け取り、ステップS101において、ライセンスデータベースを更新する。そして、ステップS102において、名簿ライセンスデータベースを更新し、ステップS103において、要求者へ訂正完了通知を送信して処理を終了する。

2. 8名簿を使用する場合の削除請求

名簿を使用する場合における情報主体の個人データを削除する手順は、2.7節の訂正請求とほぼ同様である。異なるところは、訂正の場合は、訂正した個人データに変更するが、削除の場合は、その処理はいらない。

3. サービス業者間での個人データの保護

図21は、サービス業者間で個人データを取り引きする処理を示す図である。

【0071】

サービス業者間で個人データを取り引きする場合、必ず情報主体に提供してよい旨の同意を得る必要がある。サービス業者Aが、ある情報主体の個人データを保有していると仮定し、サービス業者Bにその個人データを提供する場合を考える。

3. 1 サービス業者間におけるライセンス提供の仕組み

①個人情報提供の要求

- ・サービス業者Bは、サービス業者Aに対して個人データ提供を要求する。

②個人データ提供の同意要求

- ・サービス業者Aは、情報主体に、サービス業者Bから個人データ提供の要求が来たことを通知する。
- ・このとき、サービス業者Aは、サービス業者Bの少なくとも、以下の情報を情報主体に提供する。

【0072】

サービス業者Bの名称、連絡先

個人データの利用目的

個人データを提供したときに受けられる特典、サービス

開示・訂正・削除請求の問い合わせ先と問い合わせ方法

サービス業者Bの身元を保証する電子証明書。例えば、サービス業者Bの保有するライセンスデータベースシステムの証明書など。

③提供の意思表示

- ・情報主体は、サービス業者Aを通して、個人データをサービス業者Bへ提供するかどうかを決定する。
- ・提供する場合は、個人データ使用ライセンスを発行し、サービス業者Aへ送信する。このとき、個人データ使用ライセンスは、サービス業者Bが保有しているライセンスデータベースシステムの公開鍵を用いて暗号化される。

【0073】

このことにより、経由先のサービス業者Aでは、個人データ使用ライセンスの使用はできない。

④暗号化個人データ取得

・サービス業者Aは、情報主体から同意の通知がきた場合、サービス業者Bに暗号化個人データを送信する。

⑤ライセンス提供

・サービス業者Bは、サービス業者Aから個人データ使用ライセンスを取得する。

【0074】

図22は、サービス業者Bへの個人データ使用ライセンスを発行するときのクライアントツールの処理を示すフローチャートである。

ステップS110において、サービス業者Bからの個人データ要求（サービス業者Bの証明書を含む）をサービス業者Aから受信する。ステップS111において、情報主体は個人データを提供するか否かを判断する。ステップS111の判断がNOの場合には、ステップS112において、エラー処理を行い、処理を終了する。

【0075】

ステップS111における判断がYESの場合には、ステップS113において、個人データを作成し、ステップS114において、共通鍵方式の鍵を生成する。そして、ステップS115において、個人データを暗号化し、ステップS116において、個人データ使用ライセンスを生成する。そして、ステップS117において、暗号化した個人データを送信する。そして、ステップS118において、DRM認証する。ステップS118のDRM認証は、サービス業者Bの公開鍵を使用する。

【0076】

ステップS118のDRM認証の結果が無効の場合には、ステップS119において、エラー処理を行い、処理を終了する。ステップS118のDRM認証の結果が有効である場合には、ステップS120において、個人データ使用ライセンスをサービス業者Aへ送信して、処理を終了する。サービス業者Aへ送られた個人データ使用ライセンスは、サービス業者Bに転送される。

3. 1. 1 開示請求

図23は、サービス業者間で個人データを取り引きする場合における、サービ

ス業者Bへの開示請求の処理を説明する図である。

【0077】

情報主体がサービス業者Bに対して個人データの開示を請求するときに、サービス業者Aを介してサービス業者Bに請求する。サービス業者Aが情報主体とサービス業者Bの間にいる以外は、2.2節と同じ。

すなわち、

- ①サービス業者Bに対して、個人データの開示要求を出す。
- ②サービス業者Aを介して、サービス業者Bに、情報主体へ個人データを開示するように要求する。
- ③サービス業者Bは、暗号化個人データとサービス業者Bが作成した付加情報を情報主体に送信する。
- ④情報主体は、受信した個人データを復号する。

3.1.2 訂正請求

図24は、サービス業者間で個人データを取り引きする場合における訂正請求の処理を説明する図である。

【0078】

サービス業者Aがサービス業者Bに個人データを提供している場合、情報主体からの個人データの訂正要求に応じる処理は、次のような流れである。

情報主体は、サービス業者Aに訂正した暗号化個人データと訂正した使用ライセンスを送信する。サービス業者Aは、訂正した個人データを同期するためにサービス業者Bに訂正情報を送信する。

【0079】

すなわち、

- ①クライアントツールからサービス業者Aに個人データ訂正要求が送られる。
- ②クライアントツールは、個人データを暗号化する。
- ③暗号化個人データがクライアントツールからサービス業者Aへ送信される。
- ④サービス業者Aでは、新しい個人データで古い個人データが更新され、暗号化個人データの同一性を保つための同期処理がサービス業者Aからサービス業者Bに対して行われる。

- ⑤クライアントツールは、個人データ使用ライセンスをサービス業者Aに提供する。サービス業者Aでは、古い個人データ使用ライセンスが新しい個人データ使用ライセンスによって更新される。
- ⑥個人データ使用ライセンスの同一性を保つための同期処理がサービス業者Aからサービス業者Bに対して行われる。
- ⑦サービス業者Bは、サービス業者Aに訂正完了通知を送信する。
- ⑧サービス業者Aは、情報主体に訂正完了通知を送信する。

【 0 0 8 0 】

図 2 5 は、サービス業者間での個人データの同一性を保つための同期処理を示すフローチャートである。

ステップ S 1 3 0 において、訂正請求の要求者へ訂正完了通知を送信する。ステップ S 1 3 1 において、サービス業者Aは、サービス業者Bへ訂正要求を送信する。ステップ S 1 3 2 において、サービス業者Aは、サービス業者Bから認証を受ける。ステップ S 1 3 2 の認証の結果、無効と判断された場合には、ステップ S 1 3 3 において、拒否通知をサービス業者Aが受け取り、処理が終了する。ステップ S 1 3 2 の認証の結果、有効と判断された場合には、ステップ S 1 3 4 において、サービス業者Aは、サービス業者Bへ訂正データを送信する。ステップ S 1 3 5 において、サービス業者Bは、訂正データを D R M 認証する。

【 0 0 8 1 】

ステップ S 1 3 5 の D R M 認証において、無効と判断された場合には、ステップ S 1 3 6 において、エラー処理を行い、ステップ S 1 3 9 において、要求拒否通知を受信し、処理を終了する。ステップ S 1 3 5 において、D R M 認証の結果が有効の場合には、ステップ S 1 3 7 において、訂正した個人データ使用ライセンスを送信し、ステップ S 1 3 8 において、サービス業者Bからの訂正完了通知を受信して、処理を終了する。

3. 1. 3. 削除請求

名簿を使用する場合における情報主体の個人データを削除する手順は、3. 1. 2 節の訂正請求とはほぼ同様である。異なるところは、訂正の場合は、訂正した情報に変更するが、削除の場合は、その処理はいらないことである。

3. 2. 名簿を使用する場合

サービス業者A、サービス業者Bともに個人データを、名簿を用いて使用する場合について、情報主体から、開示・訂正・削除請求に応じる流れを説明する。

3. 2. 1 名簿を使用する場合の開示請求

3. 1. 1 節と同じ。

3. 2. 2 名簿を使用する場合の訂正請求

図 26 は、名簿を使用する場合の訂正請求の処理を説明する図である。

【0082】

サービス業者Aがサービス業者Bに名簿を提供している場合、情報主体からの個人情報の訂正要求に応じる方法は、3. 1. 2 節とほぼ同じである。

すなわち、情報主体から特定のサービス業者A、Bへ個人データを提供している状況で、情報主体が個人データの修正を要求するとき、サービス業者Aに対して、2つの個人データ使用ライセンスを発行する。個人データ使用ライセンスを発行するとき、情報主体は、サービス業者Aのために、サービス業者Aの公開鍵で暗号化した個人データライセンスと、サービス業者Bのために、サービス業者Bの公開鍵で暗号化した個人データ使用ライセンスをサービス業者Aに送信する。受け取ったサービス業者Aは、個人データ使用ライセンスをライセンスデータベースに保存し、ライセンスデータベースと名簿ライセンスデータベースを更新する。更に、サービス業者Aは、サービス業者B用の個人データ使用ライセンスをサービス業者Bへ送信し、受け取ったサービス業者Bは、サービス業者Aと同様に、名簿ライセンスデータベースを更新する。

【0083】

図 27 は、名簿を使用する場合の訂正要求におけるサービス業者Aの処理のフローチャートである。

ステップS150において、訂正請求をしてきた要求者は登録者であるか否かの認証を行う。ステップS150の認証の結果、登録者でないと判断された場合には、ステップS151において、エラー処理を行い、ステップS152において、要求拒否通知を送信して処理を終了する。

【0084】

ステップS150の認証の結果、要求者が登録者であると判断された場合には、ステップS153において、訂正データを要求する。そして、ステップS154において、訂正された暗号化データを受信し、ステップS155において、個人データ・データベースの更新を行い、ステップS156において、名簿データベースの更新を行う。

【0085】

そして、ステップS157において、個人データ使用ライセンスのDRM認証を行う。ステップS157において、無効と判断された場合には、ステップS158において、エラー処理を行い、ステップS159において、要求拒否通知を送信して処理を終了する。

【0086】

ステップS157のDRM認証において、有効と判断された場合には、ステップS160において、サービス業者A、B用の使用ライセンスを受信する。そして、ステップS161において、ライセンスデータベースを更新し、ステップS162において、名簿ライセンスデータベースを更新する。ステップS163においては、サービス業者Bからサービス業者Aが認証を受ける。ステップS163の認証が無効と判断された場合には、ステップS164において、エラー処理を行い、ステップS165において、要求拒否通知を受信し、処理を終了する。

【0087】

ステップS163の認証が有効と判断された場合には、ステップS166において、訂正された暗号データをサービス業者Bに送信し、ステップS167において、サービス業者BによってDRM認証を受ける。ステップS167のDRM認証の結果が無効の場合には、ステップS168において、エラー処理を行い、ステップS169において、要求拒否通知を受信して処理を終了する。ステップS167のDRM認証の結果が有効の場合には、ステップS170において、サービス業者B用の個人データ使用ライセンスを送信して、処理を終了する。

3. 2. 3. 名簿を使用する場合の削除請求

名簿を使用する場合における情報主体の個人データを削除する手順は、3. 2. 2節の訂正請求とほぼ同様である。異なるところは、訂正の場合は、訂正した

情報に変更するが、削除の場合は、その処理は行わないことである。すなわち、個人データと個人データ使用ライセンスを消去するだけである。

4. センタ型展開例

個人情報の提供を一手に引き受ける個人データ取り扱い事業者が、個人データセンタとなり、そのセンタが情報主体の個人データを管理し、サービス業者へ提供するという形態を考える。

【0088】

ここでは、サービス業者は、個人データのリスト（名簿）の提供を望んでいるものとする。

この展開例においてはセンタは、サービス業者と情報主体との仲介をするだけである。具体的には、あるサービス業者からセンタに個人データ提供の要求があったときに、センタは、情報主体の個人データ使用ライセンスに従って、個人データを提供しても良いかを判断し、その結果、提供する場合は、提供した後に情報主体に通知する。

[ライセンスの提供の仕方]

センタは、様々なサービス業者からの個人データ提供要求を受け付けるが、そのたびに情報主体に使用同意を取っていたのでは、情報主体にとって利便性が悪い、また、センタはサービス業者に対して早急な対応ができない。

【0089】

そこで、情報主体は、センタにライセンスを100個あるいは1000個といった、ある程度の数のライセンスを登録し、登録しておいたライセンスが無くなったときに、センタが、情報主体にライセンス登録の更新を要求する。

【0090】

そして、センタがサービス業者に使用ライセンスを提供するときには、センタは、要求してきたサービス業者の業種や情報主体へのサービス内容、また、使用目的などが、情報主体が提供した使用ライセンス属性とマッチするかで判断をして提供する。

4. 1 センタ型展開例の概要

図28は、センタ型個人データ提供システムの構成例である。

【0091】

情報主体が、個人データ使用ライセンスを自ら発行する。ここでのセンタの役割は、主に、サービス業者からの提供要求の管理と、各情報主体が、どのサービス業者へ情報提供したかのデータを管理する。

【0092】

この形態では、以下のような流れで個人情報提供が提供され使用される。

登録の流れ

1. 情報主体は、センタに登録する。
 - ・ 情報主体は、ある単位でライセンスをセンタに送信しておく。
2. センタは登録者に対して、IDを発行する。
 - ・ センタは、サービス業者からの通知を送るために、登録者のIDと連絡先（電子メールアドレス）を対にしてリストにしておく。

提供の流れ

1. サービス業者は、センタに、ある条件（例えば、20代の男性など）の個人情報（名簿）を提供するように要求する。
 - ・ このとき、サービス業者がセンタに提出するものは、「条件」と「事業者証明書」である。
 2. センタは、登録者の中から条件に該当する情報主体を検索し、提供可能な情報主体を特定する。
 3. 2の該当者の個人データからなる名簿および名簿ライセンスを作成する。
 4. センタは、暗号化名簿と名簿使用ライセンスをサービス業者に提供する。
 5. サービス業者は、受け取った名簿を使用目的の範囲で名簿を使用する。
 6. 4の該当者に対してサービス業者に個人データを提供したことを通知する。
- そのとき、少なくともサービス業者の以下の情報を提供する。

- ・ サービス業者の名称、連絡先
- ・ 個人情報の利用目的
- ・ 個人情報を提供したときに受けられる特典、サービスなど。
- ・ 開示・訂正・削除請求の問い合わせ先と問い合わせ方法。

4. 1. 1. 該当する情報主体の検索方法について

センタがサービス業者からある条件の個人データの名簿を要求されたときに、センタは、以下の条件全てに満足する個人データを探す。この処理は、名簿ライセンスデータベースの検索ツールを使って実行される。

(1) サービス業者の業種

・ サービス業者が提出する証明書に記載されている業種と情報主体が提出したライセンスの属性である提供許可業者を比較する。

【0093】

例えば、X. 509 v3 証明書では、拡張領域に事業者の業種・サービス内容などを記述しておく。

X. 509 v3 証明書は、ITU (International Telecommunications Union: 国際電気通信連合電気通信標準化部門) が定めたデジタル証明書の標準仕様である。多くの場合、X. 509 v3 という書式に従う。v3 では拡張領域を設け、証明書発行者が独自の決められた情報を追加できるようにしている。

(2) サービス業者のサービスの提供内容

・ サービス業者の証明書の情報とライセンスの属性である提供拒否サービスを比較する。

(3) サービス業者の個人データの使用目的

・ サービス業者の使用目的とライセンスの属性である使用目的を比較する。

(4) サービス業者の要求している条件 (30歳未満でスポーツが趣味など)

・ 暗号化された名簿を復号し、サービス業者の提出した条件と個人データを比較する。

(1)、(2) に関しては、それらの情報を確かめるためにサービス業者の電子証明書の中に含め、正当性を検証できるようにする。

【0094】

図29は、検索ツール処理フローチャートを示す図である。

ステップS200においては、サービス業者の証明書をロードする。ステップS201において、証明書の業種と合致する属性を持つ名簿ライセンスが存在するか否かを判断する。ステップS201における判断がNOの場合には、ステップS202において、エラー処理を行い、処理を終了する。ステップS201に

おける判断がYESの場合には、ステップS203において、合致するライセンスを残す。そして、ステップS204において、証明書にあるサービスと合致する属性を持つ名簿ライセンスが存在するか否かを判断する。ステップS204の判断がNOの場合には、ステップS204aにおいて、エラー処理を行い、処理を終了する。ステップS204における判断がYESの場合には、ステップS205において、合致するライセンスを残す。ステップS206においては、サービス業者の要求する使用目的と合致する属性を持つ名簿ライセンスが存在するか否かを判断する。ステップS206の判断がNOの場合には、ステップS206aにおいてエラー処理を行い、処理を終了する。

【0095】

ステップS206の判断において、YESと判断された場合には、ステップS207において、合致するライセンスを残し、ライセンサー名簿IDを取得する。ステップS208において、対応する暗号化された名簿をロードし、ステップS209において、名簿を復号し、ステップS210において、現在残っているライセンスに対応する個人データを残す。そして、ステップS211において、サービス業者の要求する条件を満たす個人データが存在するか否かを判断する。

【0096】

ステップS211における判断がNOの場合には、ステップS212において、エラー処理を行い、処理を終了する。ステップS211における判断がYESの場合には、ステップS213において、合致する個人データを残し、ステップS214において、残った個人データのIDと使用した名簿のライセンサー名簿IDを取得し、処理を終了する。

【0097】

以上において、ステップS200からステップS207は、ライセンスとサービス業者の証明書だけで行う処理であり、ステップS208からステップS214は、復号された個人データとサービス業者の要求条件で行う処理である。

4. 2 センタへの登録

図30は、センタへの登録処理を説明する図である。

①個人情報の運用に関する事項の通知

・個人情報センタは、情報主体に個人情報を登録してもらう際、必ず個人情報の運用についての規定を提示する。

・その内容については、必ず以下の事柄を含んでいる。

(ア) 第三者へ提供することが、利用目的であること

(イ) 第三者への提供手段・方法

(ウ) 情報主体の求めに応じて、開示・訂正・削除ができること

(エ) 情報主体の求めに応じて、このサービスの停止ができ、かつ個人情報センタの登録簿からその情報主体の情報が削除されること

(オ) 登録するときに、必要な個人情報の項目

・登録フォームも含まれている。情報主体は、このフォームに個人情報を入力する。

②フォーム要求

・情報主体が上記の内容を吟味した上で、登録したいと思ったら、個人情報センタへ登録フォームを要求する。

③フォームの提供

・個人情報主体は、フォームの要求を受けたら、登録フォームを送信する。

④個人情報の暗号化

・情報主体は、登録フォームに個人情報を入力し、フォームを暗号化するクライアントツールを使用して共通鍵暗号方式の鍵を生成し、その鍵で暗号化する。

⑤個人情報の登録

・暗号化した個人情報を個人情報センタに提供する。

⑥登録者のリストを作成

・個人データ管理ツールは、登録者に登録者識別子（ID）を発行し、そのIDと電子メールアドレスを対にしたリストを作成する。

・このリストは、各登録した情報主体と、その情報主体が個人情報を提供したサービス業者の情報を関連付けたリストとなる。表3参照。

【0098】

【表 3】

業者名	業種	サービス 内容	住所	問い合わせ先	提供項目	利用 目的
〇〇株式会社	メーカー	---	〇〇〇〇〇	〇〇-□□□	氏名/性別/生年月日/住所/メールアドレス/ 興味のある分野/	市場調査/
△△△	情報処理	---	△△△△△	〇〇-△△△	氏名/性別/生年月日/趣味	市場調査/
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・
××保険	金融	---	××××××	〇〇-×××	氏名/性別/生年月日/住所/収入/	広告

【0099】

・このリストは、サービス業者から要求があった場合に、登録者（情報主体）に通知するために用いられる。また、登録者から開示・訂正・削除請求をするため、その人が、どのサービス業者に情報を提供しているかを確認する目的で使用される。

⑦ライセンスを提供

・情報主体は、暗号化個人情報と、センタ側でサービス業者が要求する条件の個人データを検索するための検索用ライセンスとある単位の使用ライセンスを登録する。

なお、⑦の個人データ管理ツールとは、以下のようなもの。

[個人データ管理ツール]

個人情報取扱事業者が、個人データを第三者に提供するとき、個人情報取扱事業者は、表3のような情報主体別に、その情報主体の個人情報をどの事業者を提供したかの一覧を管理する。個人データ管理ツールとは、このような情報主体別にその個人情報を提供した事業者のリストを生成するツールのことである。また、このツールは、情報主体の個人情報を一切使用しないので、DRM機能は必要ない。

4. 3 個人データの提供

図31は、個人データの提供処理を説明する図である。

①個人情報提供要求

- ・サービス業者は個人情報センタへ個人情報名簿の提供を要求する。
- ・具体的には、サービス業者は20代の男性などある条件の名簿を要求する。

・ サービス業者の（業種・サービス内容などの企業情報の）証明書を提出する。

②該当者を検索

・ 個人情報センタは、検索ツールを用いて、サービス業者が要求している該当の情報主体を 1. 1. 1 節の方法で検索する。

・ 検索ツールは、暗号化個人情報と検索用ライセンスとサービス業者の要求条件と事業者証明書が入力され、該当の ID のリストが出力される。

③名簿を作成する

・ 個人情報センタは、第三者提供に対し、名簿作成ツールを使用して、②に該当する情報主体の個人情報からなる暗号化名簿とその名簿の使用ライセンスを作成し、各々名簿データベースシステム、名簿使用ライセンスデータベースシステムに保存する。

④名簿の提供

・ 個人情報センタは、暗号化名簿と名簿ライセンスをサービス業者へ提供する。

⑤提供先リストを更新する

・ 個人データ管理ツールは、③で作成された名簿に載っている情報主体に対して提供先リストの更新をする。

⑥提供通知

・ 個人情報センタは、各情報主体に対してサービス業者へ個人情報を提供したことを通知する。

・ このとき、センタは、サービス業者に関する少なくとも以下の情報を通知する。

【0100】

サービス業者の名称、連絡先

個人情報の利用目的

個人情報を提供したときに受けられる特典、サービスなど。

【0101】

開示・訂正・削除請求の問い合わせ先と問い合わせ方法。

図 32 は、センタの提供処理フローチャートである。

ステップ S220 において、サービス業者の証明書の検証を行う。ステップ S

221において、無効と判断された場合には、ステップS222において、エラー処理を行い、処理を終了する。ステップS221において、有効と判断された場合には、ステップS223において、検索ツールで該当者を検索する。ステップS223において、該当者がいないと判断された場合には、ステップS224において、サービス業者に通知し、処理を終了する。ステップS223において、該当者がいると判断された場合には、ステップS225において、名簿作成ツールで名簿と名簿使用ライセンスを作成する。そして、ステップS226において、名簿と名簿使用ライセンスをデータベースに保存し、ステップS227において、作成した暗号化された名簿のコピーをサービス業者に送信する。そして、ステップS228において、DRM認証し、ステップS228のDRM認証が無効の場合には、ステップS229において、エラー処理して処理を終了する。ステップS228のDRM認証が有効と判断された場合には、ステップS230において、作成した名簿ライセンスを送信し、ステップS231において、作成した名簿に載っている情報主体の提供先リストを更新する。そして、ステップS232において、情報主体に提供したことを通知して、処理を終了する。

【0102】

図33は、名簿作成ツールのフローチャートである。

ステップS250において、検索ツールから該当のライセンサー名簿IDと個人データIDを取得する。ステップS251において、名簿データベースへ該当の暗号化名簿をロードする。ステップS252において、暗号化名簿を作成し、ステップS253において、作成された暗号化名簿を名簿データベースに保存する。そして、ステップS254において、名簿ライセンスを作成して、処理を終了する。

【0103】

図34は、提供される名簿ライセンスの作成の概略を示す図である。名簿ライセンスデータベースに保存されているデータから所定の条件を満たすデータのみを取り出し、データが取り出された後の名簿ライセンスとデータを取り出して作った名簿ライセンスとができる。データを取り出して作った名簿ライセンスは、名簿作成ツールで作成され、ユーザに提供される。

4. 4 開示請求

開示請求は、基本的には、暗号化個人データとそれに付随する情報を情報主体に送信することなので、2. 2 節及び3. 1. 1 節と同じようになる。

【0104】

ただし、センタ型モデルの場合は、個人情報管理ツールが作成したリストを暗号化個人データと一緒に情報主体に提供する。

4. 5 訂正請求

図35は、訂正請求の処理の流れを説明した図である。

【0105】

情報主体は、個人データを個人データセンタとサービス業者に渡しているが、いずれにしても情報主体は、センタに訂正要求すれば、提供した全てのサービス業者に訂正が反映される。

(1) 訂正要求

- ・情報主体は、個人情報センタに個人情報の訂正を要求する。

(2) 訂正した暗号化個人データを送信

- ・情報主体は、訂正した個人データを暗号化し、その暗号化個人データを個人情報センタに送信する。個人データの暗号化に関しては、訂正する項目について新たに共通鍵暗号方式の暗号化鍵を生成し、それを使用する。

(3) 個人データの訂正

- ・センタは、個人情報データベースにある情報主体の古い個人データを削除し、新しい暗号化個人データに更新する。

(4) 訂正すべき名簿の検索

- ・訂正を要求した情報主体が関係している名簿を個人データ管理ツールで検索する。

(5) 名簿の訂正

- ・名簿作成ツールを用いて暗号化名簿を作成し直し、更新された暗号化名簿を名簿データベースシステムに保存する。

(6) 暗号化個人データの同期

- ・サービス業者は、訂正した暗号化名簿をサービス業者の名簿データベースシス

テムと同期するために、訂正した暗号化名簿を送信する。

(7) 訂正したライセンスを送信

・情報主体は、(2) で使用した暗号鍵をライセンスの中に入れ、新しい使用ライセンスを作成し、ライセンスをセンタへ送信する。

(8) ライセンスの訂正

・センタは、ライセンスデータベースシステムの中で、古い情報主体のライセンスを削除し、受け取った使用ライセンスに更新する。

(9) 名簿ライセンスの訂正

・名簿作成ツールを用いて名簿ライセンスを作成し直し、更新された名簿ライセンスを名簿ライセンスデータベースシステムに保存する。

(10) 名簿ライセンスの同期

・サービス業者は、訂正した名簿ライセンスをサービス業者の名簿ライセンスデータベースシステムと同期するために、訂正した名簿ライセンスを送信する。

(11) 訂正完了通知

・個人情報センタは、訂正が完了したことを情報主体に通知する。

【0106】

図36は、名簿使用時のサービス業者の訂正同期処理フローチャートである。

ステップS260において、要求者へ訂正完了通知送信がされ、ステップS3261において、訂正した名簿を使用している事業者は存在するか否かが判断される。ステップS261において、存在しないと判断された場合には処理を終了する。ステップS261において、存在すると判断された場合には、ステップS262において、事業者へ訂正要求を送信し、ステップS263において、サービス事業者からユーザ認証を行う。ステップS263の結果、無効の場合には、ステップS264において、拒否通知が受信され、処理を終了する。

【0107】

ステップS263の結果、有効と判断された場合には、サービス業者へ訂正データを送信し、ステップS266において、DRM認証する。ステップS266のDRM認証の結果が無効の場合には、ステップS267において、エラー処理を行い、ステップS268において、要求拒否通知の受信が行われ、処理を終了

する。ステップ S 2 6 6 において、D R M 認証の結果、有効と判断された場合には、ステップ S 2 6 9 において、訂正した使用ライセンスを送信し、ステップ S 2 7 0 において、事業者からの訂正完了通知を受信し、ステップ S 2 7 1 において、訂正した名簿を使用している事業者は存在するか否かを判断する。ステップ S 2 7 1 において、N O と判断された場合には、処理を終了するが、Y E S と判断された場合には、ステップ S 2 6 2 に戻る。

4. 6. 削除請求

情報主体からの削除要求には、次の 2 つがある。

- (1) サービス業者が保持している名簿から個人データを削除する。
- (2) 個人情報センタが保持しているデータベースから削除する。これは、センタからのサービスの停止である。

4. 6. 1. サービス業者の中のデータの削除

図 3 7 は、サービス業者が有する個人データの削除処理を説明する図である。

【0108】

情報主体が、あるサービス業者だけからサービスを停止する場合の流れを以下に示す。

①削除要求

- ・情報主体は、特定のサービス業者 A に対して個人データの削除を要求する。

②削除要求通知

- ・個人情報センタは、サービス業者 A に情報主体から削除を要求されていることを通知する。

③名簿／名簿ライセンスの訂正

- ・個人情報センタは、名簿作成ツールを用いて、サービス業者 A に提供している名簿と名簿ライセンスを訂正する。
- ・具体的には、サービス業者に提供している暗号化された名簿から要求している情報主体の個人データを削除し、名簿ライセンスからその情報主体の使用ライセンス鍵を削除し、名簿ライセンスを更新する。

④訂正した名簿を送信する

- ・サービス業者 A は、これまで使用していた名簿を名簿データベースから削除し

、訂正された名簿を名簿データベースに保存する。

⑤訂正した名簿ライセンスを送信する。

・サービス業者Aは、これまで使用していた名簿ライセンスを名簿ライセンスデータベースから削除し、訂正された名簿ライセンスを名簿ライセンスデータベースに保存する。

⑥削除完了通知

・個人情報センタは、情報主体にすべての処理が終わったことを通知する。

4. 6. 2. センタの有する個人データの削除

図38は、センタの有する個人データの削除処理を説明する図である。

【0109】

個人情報センタの提供要求通知サービスを停止する流れを以下に示す。

①削除要求

・情報主体は、センタに個人情報の削除（センタからのサービスの停止）を要求する。

②暗号化個人データの削除

・個人情報センタは、要求している情報主体の暗号化個人データを削除する。

③使用ライセンス削除

・個人情報センタは、要求している情報主体の使用ライセンスを削除する。

④訂正すべき名簿の検索

・個人情報センタは、個人データ管理ツールを用いて、要求している情報主体に関係する名簿を検索する。

⑤訂正すべき名簿とそのライセンスを収集

⑥名簿／名簿ライセンスの訂正

・個人情報センタは、名簿作成ツールを用いて名簿と名簿ライセンスを訂正する。

・具体的には、名簿から要求している情報主体の情報を削除し、名簿ライセンスに含まれている情報主体の鍵も削除する。

⑦訂正した名簿を送信する

・個人情報センタは、訂正した名簿をサービス業者へ送信し、サービス業者は、

名簿データベースシステムにある以前の名簿を削除し、訂正された名簿に更新する。

⑧訂正した名簿ライセンスを送信する

・個人情報センタは、訂正した名簿ライセンスをサービス業者へ送信し、サービス業者は、名簿ライセンスデータベースシステムにある以前の名簿ライセンスを削除し、訂正された名簿ライセンスに更新する。

⑨削除完了通知

・個人情報センタは、情報主体に全ての処理が終わったことを通知する。

4. 7 センタ型におけるビジネスの一形態

図 39 は、センタ型ビジネスの一形態における情報主体、センタ、業者の関係を示す図である。

【0110】

個人情報センタが中心となり情報主体、サービス業者にサービスを提供するビジネス形態を考える。

4. 7. 1 情報主体と個人情報センタの関係

- ・情報主体は、センタに個人情報を提供する。
- ・センタは、情報主体が登録する際にポイントを与える。
- ・センタは、サービス業者に個人データを提供するときにポイントを与える。
- ・情報主体は、ある程度ポイントが貯まったら、商品および現金と交換できる。

[ポイントの加算方法について]

センタは、登録している情報主体に対して以下の時にポイントを加算する。

- ・情報主体が個人情報センタに個人データを登録するとき。

【0111】

・個人データを提供するとき、情報主体は、暗号化個人データとその使用ライセンスを提供する。使用ライセンスは、情報主体しか発行できないので最初に 100 個なり 1000 個なりを提供しておく。

【0112】

・センタは、ライセンスがなくなったとき、情報主体にライセンスの発行を要求する。

- ・センタが個人データをサービス業者に提供するとき

なお、ポイントの加算方法などは、例えば、表4のように設定する。

【0113】

【表4】

		ポイント（情報主体向け）	料金（事業者向け）
使用期限		100 ポイント/半年	1000 円/半年
移動回数		10 ポイント/移動回数	100 円/移動回数
使用目的	調査	5 ポイント	50 円
	貸与・販売	10 ポイント	100 円
	マイニング	7 ポイント	70 円
	・ ・ ・	・ ・ ・	・ ・ ・

【0114】

4. 7. 2 センタとサービス業者の関係

- ・センタは個人データをサービス業者へ提供する。
- ・サービス業者は、センタに個人データの使用料金を支払う。

【0115】

サービス業者から名簿提供の要求がきたときに、個人情報センタは、暗号化名簿と名簿使用ライセンスを提供する。そのとき、個人情報センタは、サービス業者の名簿の使用に対して料金を徴収する。ただし、実際には、暗号化名簿は、一旦名簿データベース上に保存されればよいので、サービス業者は、初めてセンタに名簿を要求するときにだけ提供される。したがって、その後のサービス業者からの名簿要求は、名簿ライセンスだけになる。ただし、情報主体からセンタへ個人データの訂正があった場合、センタは、個人データの同期をするために個人データベースを送信することがある。

【0116】

個人情報センタは、ライセンスをサービス業者へ提供するとき、ライセンス料計算装置と課金システムによりライセンス使用金額が計算される。ライセンス価値計算装置とは、発行された使用ライセンスを数値（金額やポイント）に変換す

る装置である。課金システムは、金額データを集計して請求金額を計算するシステムである。

4. 7. 3 情報主体とサービス業者

- ・サービス業者は、情報主体にサービスを提供する
- ・情報主体は、サービス業者にサービス料金を支払う。

4. 7. 4 ライセンスの価格設定について

ライセンスは、その利用条件によりポイント・金額が変わると考えた方が自然である。例えば、同じ暗号化個人データに関して、その使用ライセンスの期限属性が1日と1ヶ月とを比べた場合、やはり1ヶ月の使用ライセンスの方が価値が高いと考えられる。このような使用ライセンスの使用条件による値段の価値基準は、予め個人情報センタが定めるか、あるいはサービス業者とセンタが話し合いなどして決定する。例えば、表4のようなポイント及び料金体系を定める。ただし、料金・ポイントは、センシティブな個人データになれば、当然ポイント・料金体系も変化する。

4. 7. 5 ビジネス形態の処理の流れ

データの流れ

図40は、データの流れを示す図である。

【0117】

個人情報センタ、サービス業者は、すでに暗号化個人データを保有していると仮定し、情報主体は、センタが提供するサービスに登録していると仮定する。このときの情報主体からセンタを通じサービス業者までの一連のデータの流れを以下に示す。

①ライセンスの送信

- ・情報主体は、センタに登録する際、使用ライセンスを送信する。

②ライセンスの価値をポイントに換算

- ・センタのライセンス料計算装置により、受信した使用ライセンスが何ポイントになるか計算する。

③ポイント加算

- ・②で計算したポイントをポイントデータベースの累積ポイントと加算し、ポイ

ントを更新する。

④ライセンス提供

- ・センタは、要求のあったサービス業者へ使用ライセンスを送信する。
- ・ライセンスデータベースシステムにライセンスの送受があった場合、トランザクションデータベースに記録される。

⑤ライセンスの価値を料金に換算

- ・センタのライセンス料計算装置により、送信した使用ライセンスのポイント数と料金を計算する。このポイント数は、その情報主体の累積ポイントに加算される。
- ・サービス業者のライセンス料計算装置により、受信した使用ライセンスの料金を計算する。

⑥料金加算

- ・⑤で計算された料金は、センタ、サービス業者各々の課金システムに加算される。

⑦料金集計

- ・センタの課金システムは、金額データを集計して請求金額を計算する。

⑧料金の請求

- ・課金システムは、センタが契約している銀行に料金を請求する。

【0118】

(付記1) 暗号化された個人データを受信するステップと、
暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信するステップと、

前記復号鍵と個人データ使用ライセンスを復号するステップと、

前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断するステップと、

前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号するステップとを有することを特徴とする個人データ保護流通方法。

【0119】

（付記 2）前記復号鍵と個人データ使用ライセンスは D R M 認証技術を用いて暗号化及び復号化されることを特徴とする付記 1 に記載の個人データ保護流通方法。

【 0 1 2 0 】

（付記 3）前記個人データ使用ライセンスを D R M 認証技術を用いて復号化するための機構は、T R M 化されていることを特徴とする付記 2 に記載の個人データ保護流通方法。

【 0 1 2 1 】

（付記 4）前記個人データ使用ライセンスの使用条件には、該個人データ使用ライセンスの有効期限、使用可能回数、使用目的、移動回数のいずれかを少なくとも含むことを特徴とする付記 1 に記載の個人データ保護流通方法。

【 0 1 2 2 】

（付記 5）前記使用目的は、前記個人データを使用するアプリケーションの限定を含むことを特徴とする付記 4 に記載の個人データ保護流通方法。

（付記 6）前記暗号化された個人データ及び該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを複数の情報主体より受信するステップと、

複数の前記個人データ使用ライセンスを同一な条件の単位で連結して名簿ライセンスを作成するステップと、

該名簿ライセンスの作成に使用された個人データ使用ライセンスに対応する、暗号化された個人データを連結して名簿を作成するステップを有することを特徴とする付記 1 に記載の個人データ保護流通方法。

【 0 1 2 3 】

（付記 7）前記暗号化された個人データは該個人データを送信した情報主体が有する復号鍵によって復号可能となっていることを特徴とする付記 6 に記載の個人データ保護流通方法。

【 0 1 2 4 】

（付記 8）前記個人データを他の情報装置に提供する場合には、前記個人データの情報主体ごとに提供した他の情報装置を管理する組織の名称、業種、使用

目的、問い合わせ先、提供した個人データベースの項目リストのうち少なくとも一つを作成し、必要に応じて対応する情報主体に開示することを特徴とする付記 6 に記載の個人データ保護流通方法。

【0125】

(付記 9) 前記暗号化された個人データ及び該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスの少なくとも一つに訂正がある場合に、前記訂正された内容を受信するステップと、

該訂正された内容を他の情報装置に送信して、個人データ及び個人データ使用ライセンスの同一性を確保するステップとを有することを特徴とする付記 8 に記載の個人データ保護流通方法。

【0126】

(付記 10) 暗号化された個人データを受信するステップと、

暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信するステップと、

前記復号鍵と個人データ使用ライセンスを復号するステップと、

前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断するステップと、

前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号するステップとをコンピュータに実行させることを特徴とする個人データ保護流通プログラム。

【0127】

(付記 11) 暗号化された個人データを受信する手段と、

暗号化された、該個人データを復号するための復号鍵と該個人データの使用条件を記述した個人データ使用ライセンスを受信する手段と、

前記復号鍵と個人データ使用ライセンスを復号する手段と、

前記個人データの用途が前記個人データ使用ライセンスに記述された使用条件と一致するかを判断する手段と、

前記個人データの用途が前記使用条件と一致するときのみに前記復号された復号鍵を用いて前記個人データを復号する手段とを有することを特徴とする個人デ

ータ保護流通装置。

【0 1 2 8】

【発明の効果】

本発明によれば、社内での個人情報管理規定について詳細に決めていなくても、（少なくとも特定の従業員だけが、個人データ・データベースへのアクセス権を持つようにすることは必要であるが）個人データは、不正の使用、目的外使用から保護される。

【0 1 2 9】

情報主体は、提供する個人データ取扱事業者が世間一般に特別信頼されていなくても、本発明によれば、サーバ装置を設置して有れば、安心して個人データを提供することができる。

【図面の簡単な説明】

【図 1】

情報主体、事業者、第三者の関係を説明する図である。

【図 2】

本発明の実施形態の構成の概略構成を説明する図である。

【図 3】

情報主体が個人情報を提供することに同意した場合の提供の仕組みと、サービス業者がその情報を利用する仕組みを示す図である。

【図 4】

使用条件と個人データの使用との関係を説明する図である。

【図 5】

DRM認証を説明する図である。

【図 6】

クライアントツールの個人データ使用ライセンスの送信時のフローチャートである。

【図 7】

個人データと個人データ使用ライセンスとの関係を説明する図である。

【図 8】

アプリケーションで個人データを使用する際のフローチャートである。

【図 9】

ライセンスデータベースシステムのライセンス送信時のフローチャートである。

【図 10】

本発明の実施形態の別の構成における適用例を説明する図である。

【図 11】

情報主体から開示請求があった場合の開示の仕組みを示す図である。

【図 12】

情報主体からの個人データの訂正請求における動作を説明する図である。

【図 13】

サービス業者側の個人データの訂正処理のフローチャートである。

【図 14】

ライセンス代理提供サーバによる個人データの削除処理を説明する図である。

【図 15】

名簿ライセンスの生成処理を説明する図である。

【図 16】

名簿の作成と名簿ライセンスの生成処理を図示した模式図である。

【図 17】

名簿作成ツールが名簿・名簿ライセンスを作成する処理のフローチャートである。

【図 18】

名簿の使用形態を説明する図である。

【図 19】

名簿使用時の訂正要求の処理を説明する図である。

【図 20】

名簿使用時のサービス業者の名簿の訂正処理を示すフローチャートである。

【図 21】

サービス業者間で個人データを取り引きする処理を示す図である。

【図 2 2】

サービス業者 B への個人データ使用ライセンスを発行するときのクライアントツールの処理を示すフローチャートである。

【図 2 3】

サービス業者間で個人データを取り引きする場合における、サービス業者 B への開示請求の処理を説明する図である。

【図 2 4】

サービス業者間で個人データを取り引きする場合における訂正請求の処理を説明する図である。

【図 2 5】

サービス業者間での個人データの同一性を保つための同期処理を示すフローチャートである。

【図 2 6】

名簿を使用する場合の訂正請求の処理を説明する図である。

【図 2 7】

名簿を使用する場合の訂正要求におけるサービス業者 A の処理のフローチャートである。

【図 2 8】

センタ型個人データ提供システムの構成例である。

【図 2 9】

検索ツール処理フローチャートを示す図である。

【図 3 0】

センタへの登録処理を説明する図である。

【図 3 1】

個人データの提供処理を説明する図である。

【図 3 2】

センタの提供処理フローチャートである。

【図 3 3】

名簿作成ツールのフローチャートである。

【図 3 4】

提供される名簿ライセンスの作成の概略を示す図である。

【図 3 5】

訂正請求の処理の流れを説明した図である。

【図 3 6】

名簿使用時のサービス業者の訂正同期処理フローチャートである。

【図 3 7】

サービス業者が有する個人データの削除処理を説明する図である。

【図 3 8】

センタの有する個人データの削除処理を説明する図である。

【図 3 9】

センタ型ビジネスの一形態における情報主体、センタ、業者の関係を示す図である。

【図 4 0】

データの流れを示す図である。

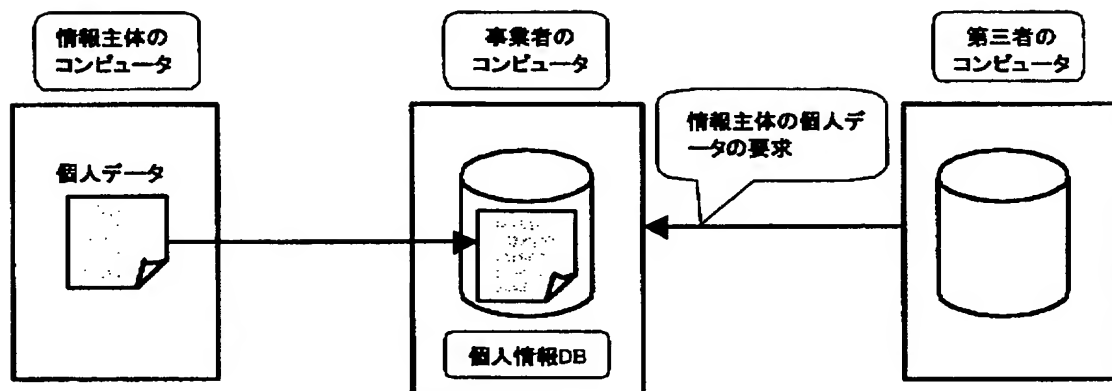
【符号の説明】

- 1 0 個人データ
- 1 1 復号鍵
- 1 2 個人データ使用ライセンス
- 1 3、1 5 セッション鍵
- 1 4 公開鍵暗号方式の鍵
- 2 0 情報主体／クライアントツール
- 2 1 サービス業者のコンピュータ
- 2 2 個人データ・データベースシステム
- 2 3 ライセンスデータベースシステム
- 2 4 アプリケーション
- 2 5 ネットワーク

【書類名】 図面

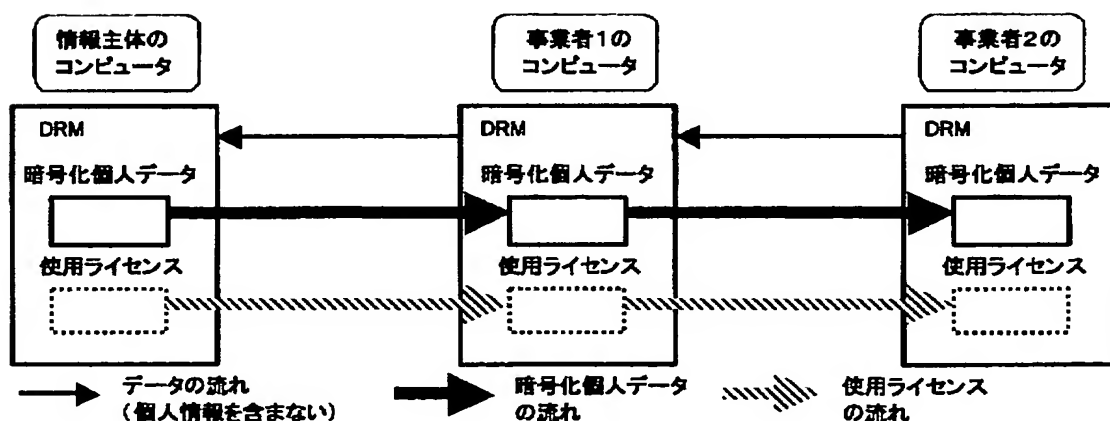
【図 1】

情報主体、事業者、第三者の関係を説明する図



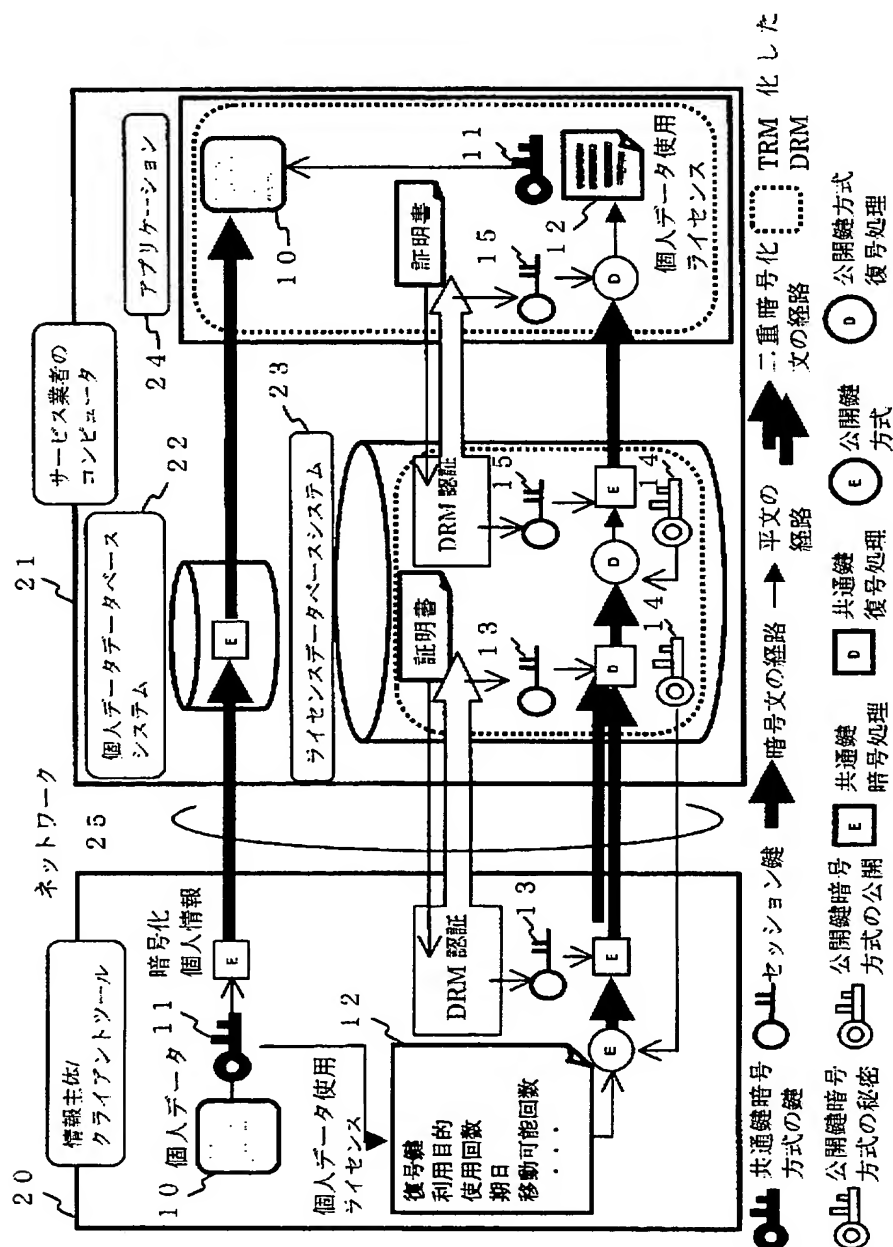
【図 2】

本発明の実施形態の構成の概略構成を説明する図



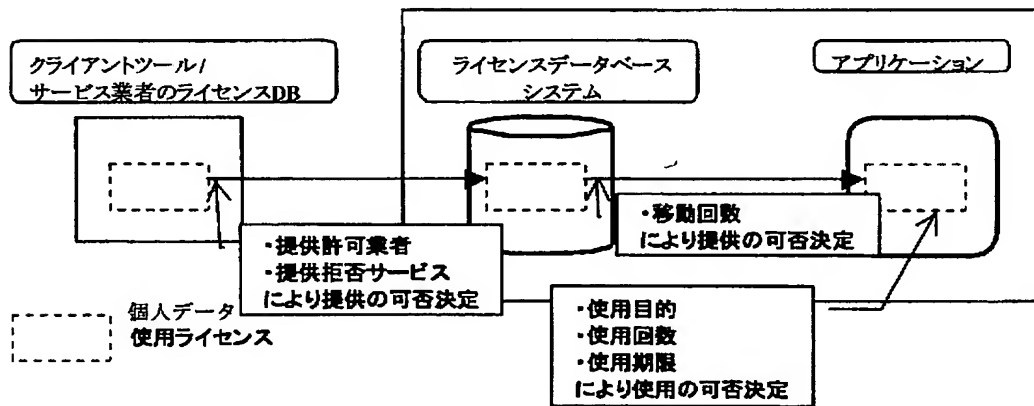
【図 3】

情報主体が個人情報を提供することに同意した場合の提供の仕組みと、サービス業者がその情報を利用する仕組みを示す図



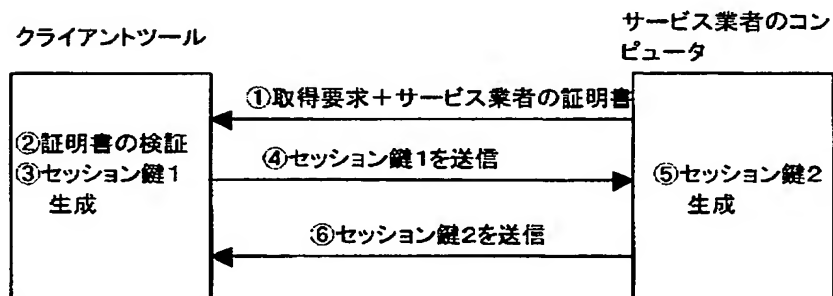
【図 4】

使用条件と個人データの使用との関係を説明する図

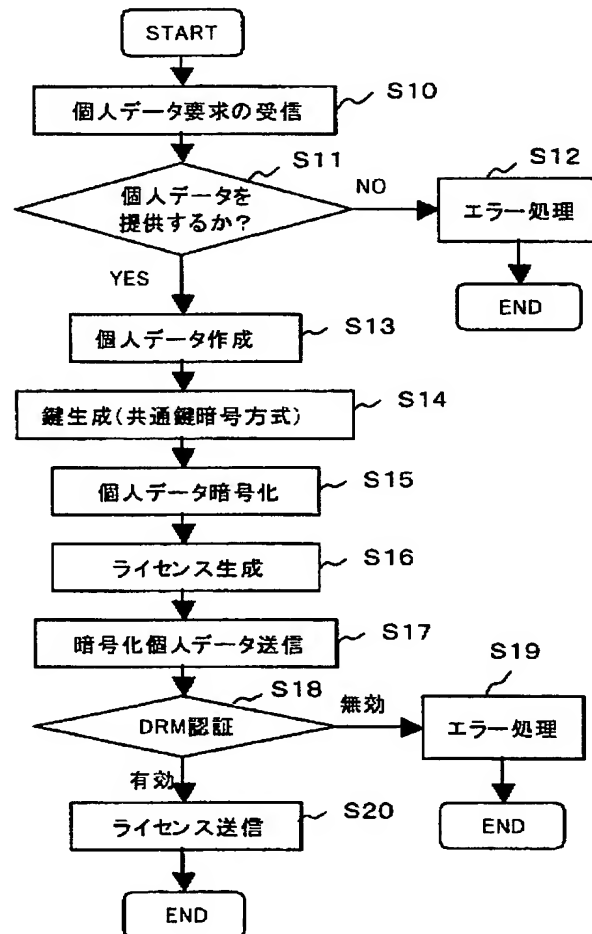


【図 5】

DRM認証を説明する図

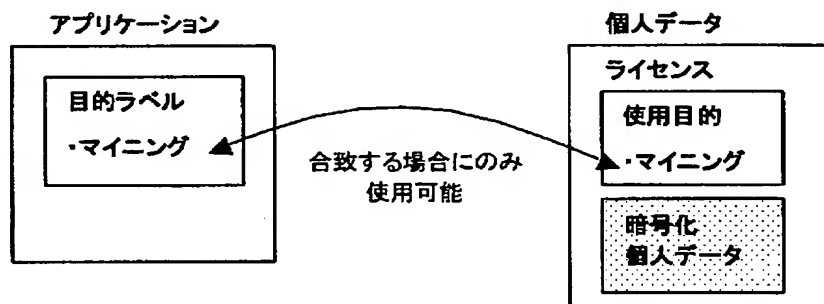


【図 6】

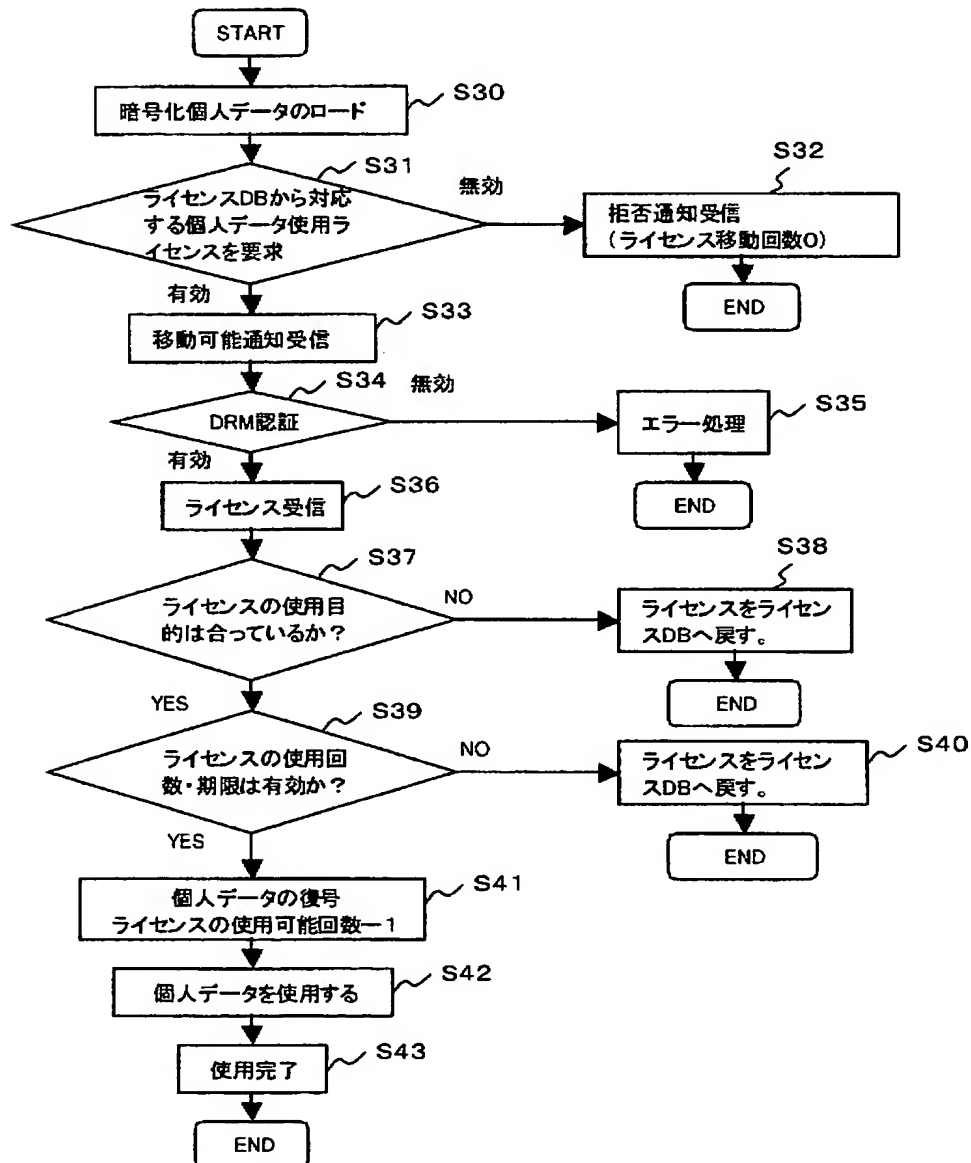
情報主体のコンピュータにおいてクライアントツールの
個人データ使用ライセンスの送信時のフローチャート

【図 7】

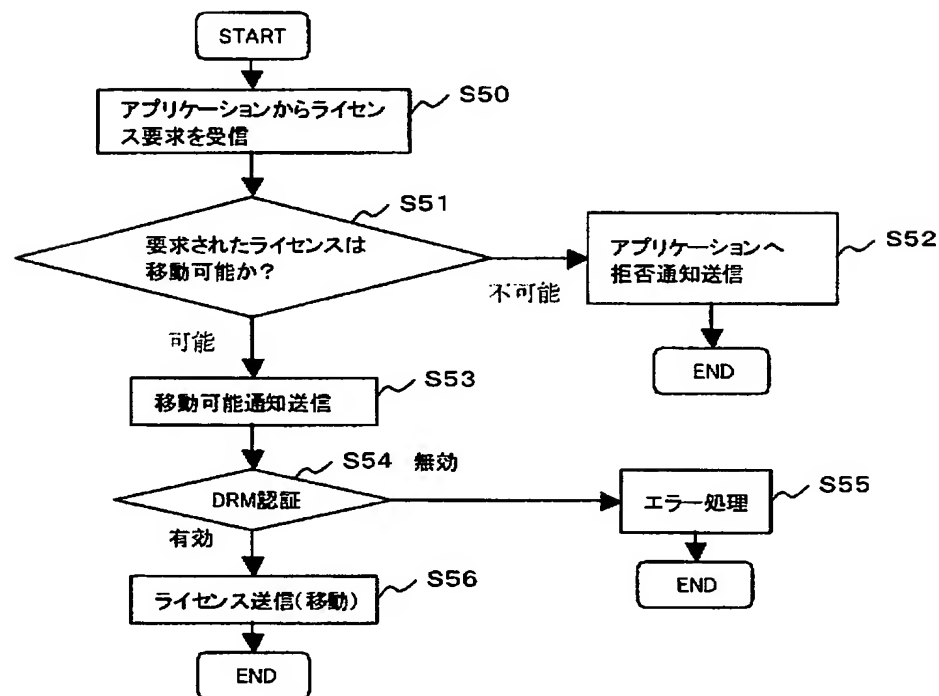
個人データと個人データ使用ライセンスとの関係を説明する図



【図 8】

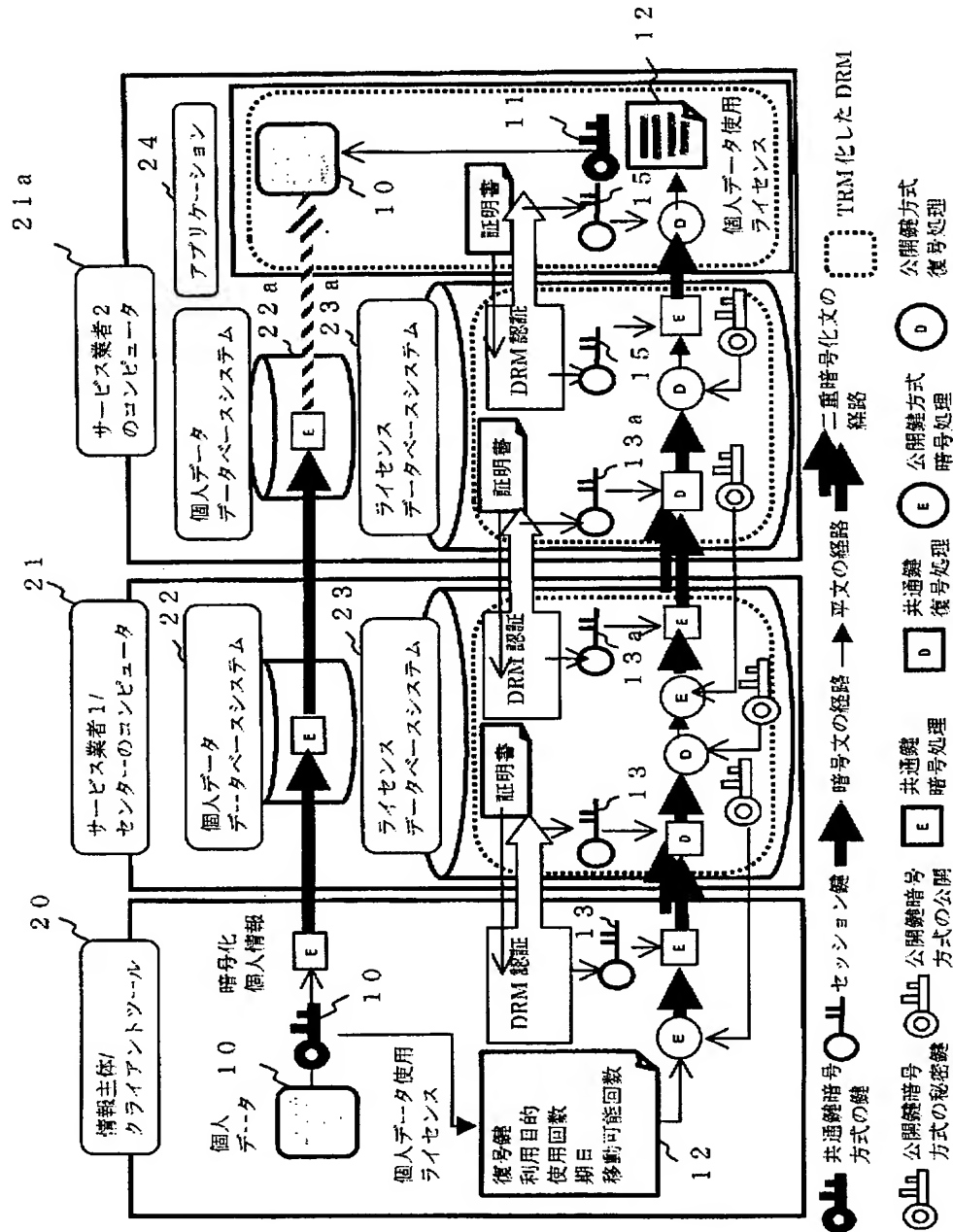
サービス業者のアプリケーションで
個人データを使用する際のフローチャート

【図 9】

ライセンスデータベースシステムの
ライセンス送信時のフローチャート

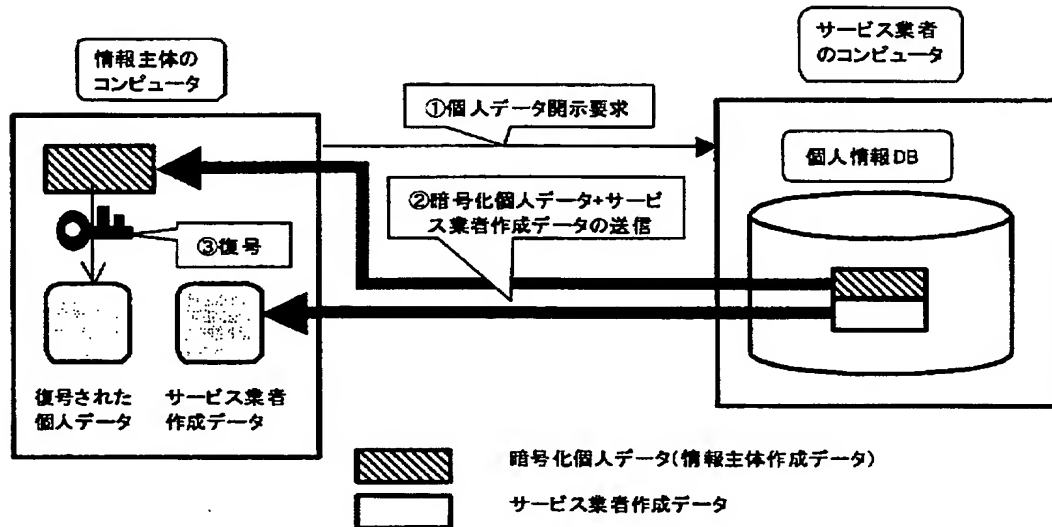
【図10】

本発明の実施形態の別の構成における適用例を説明する図



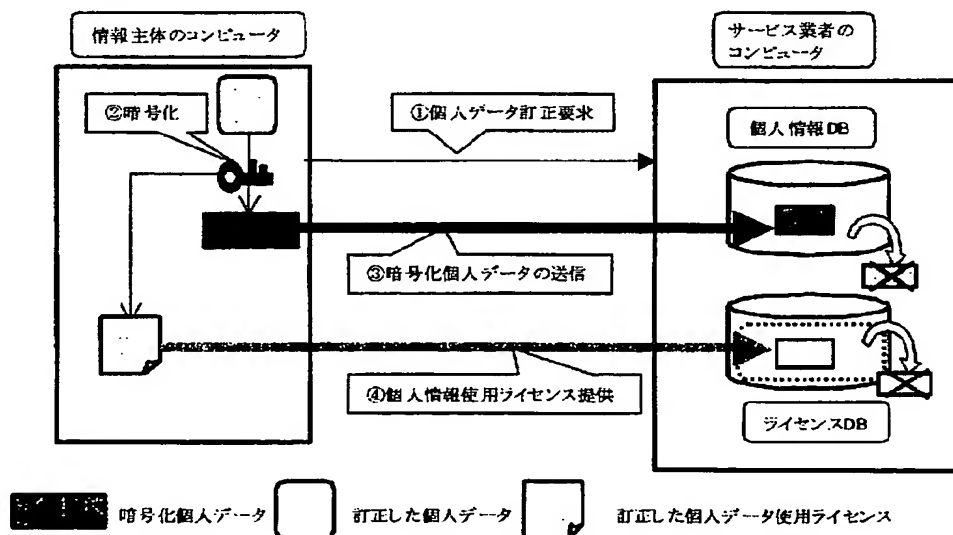
【図 11】

情報主体から開示請求があった場合の開示の仕組みを示す図



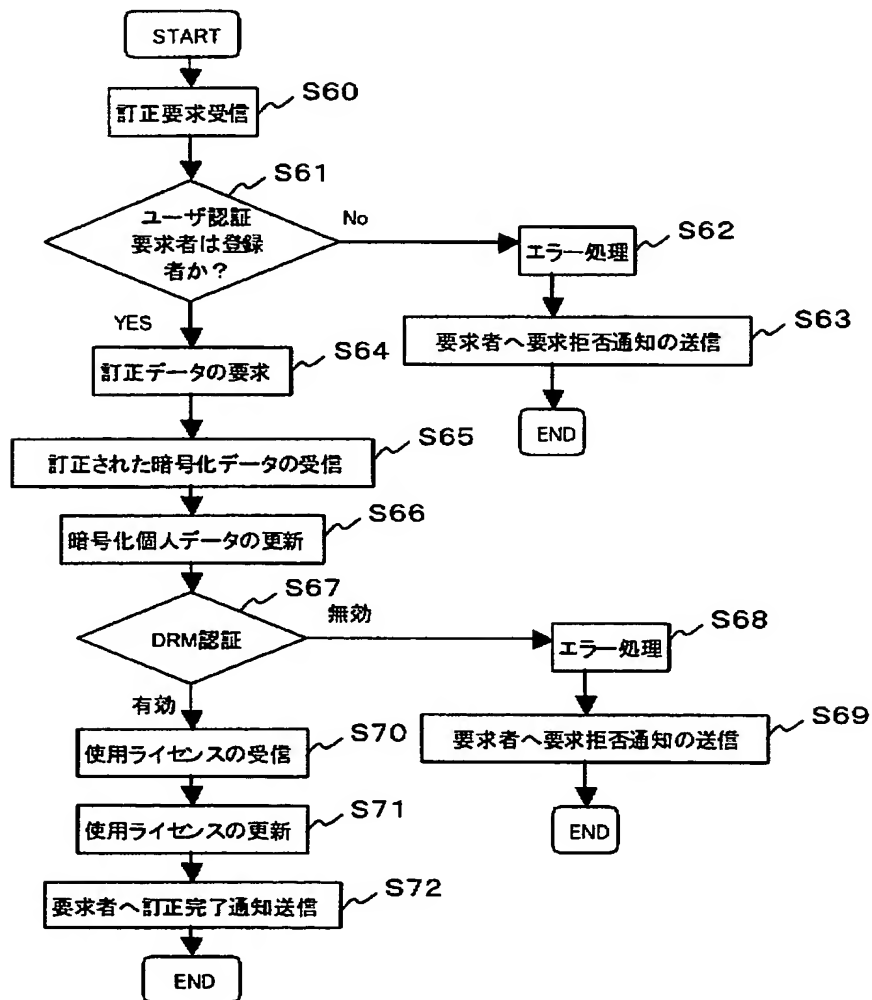
【図 12】

情報主体からの個人データの訂正請求における動作を説明する図



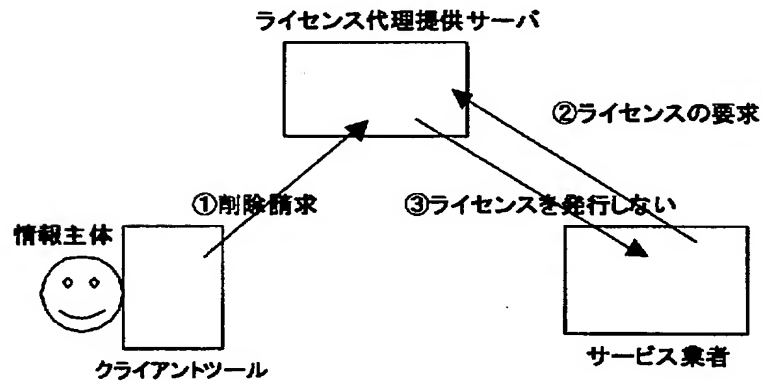
【図 13】

サービス業者側の個人データの訂正処理のフローチャート



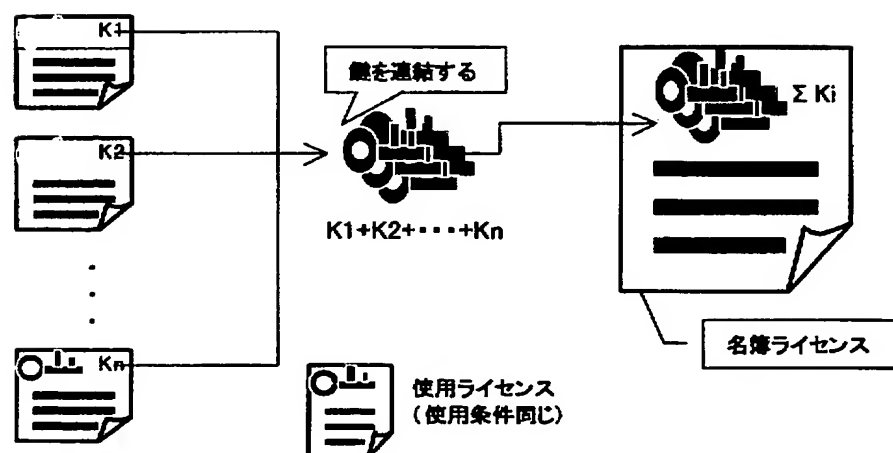
【図 14】

ライセンス代理提供サーバによる 個人データの削除処理を説明する図



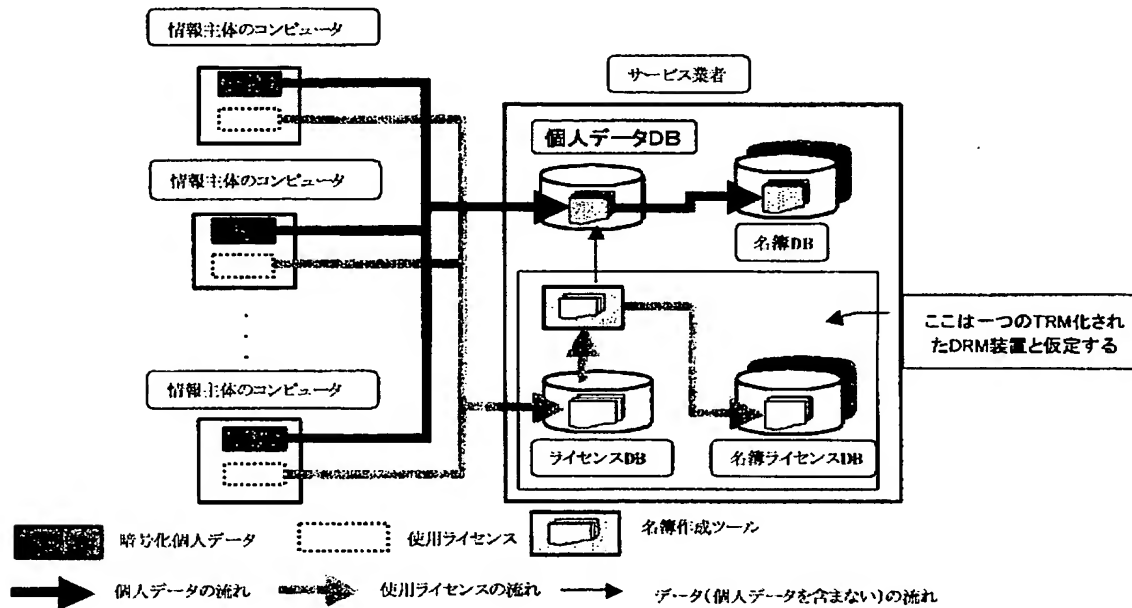
【図 15】

名簿ライセンスの生成処理を説明する図



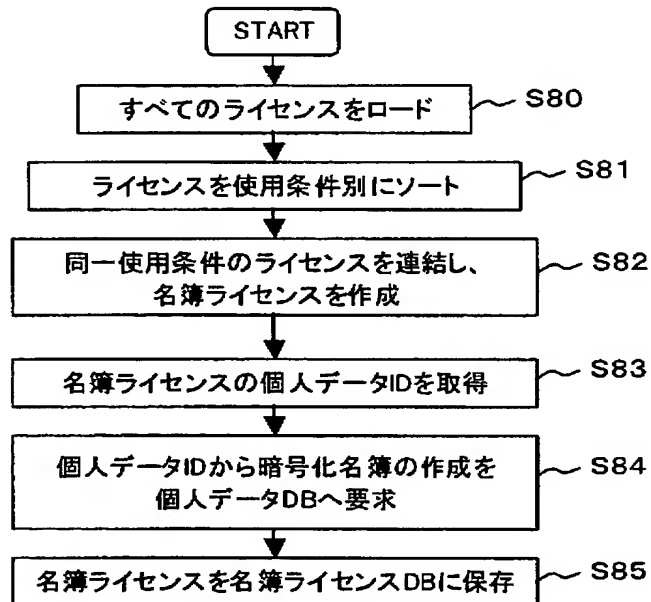
【図 16】

名簿の作成と名簿ライセンスの生成処理を図示した模式図



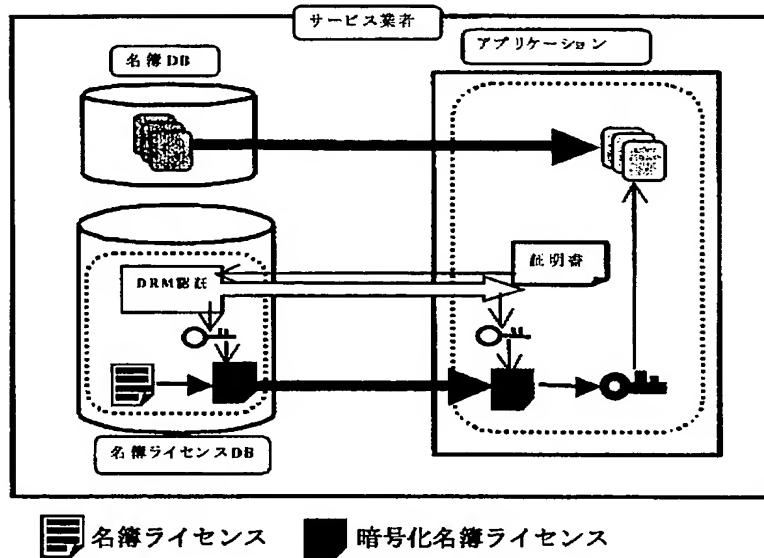
【図 17】

名簿作成ツールが名簿・名簿ライセンスを作成する 処理のフローチャート



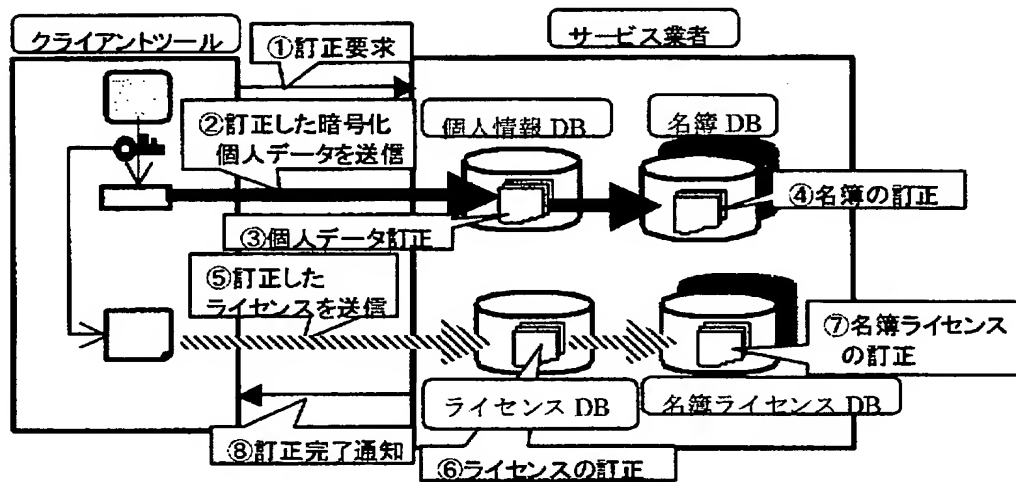
【図 18】

名簿の使用形態を説明する図

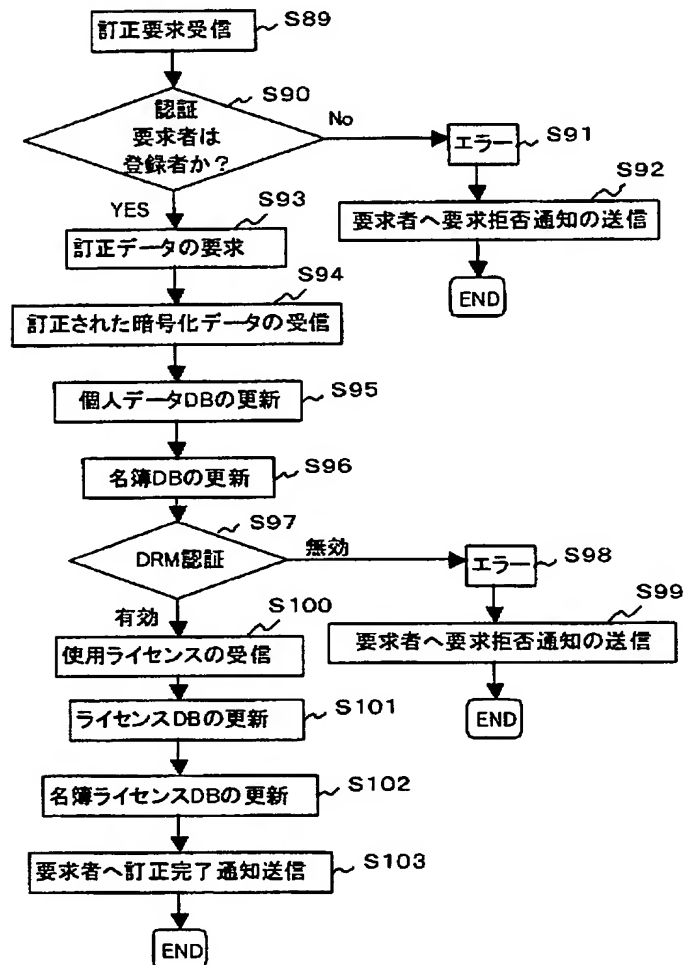


【図 19】

名簿使用時の訂正要求の処理を説明する図

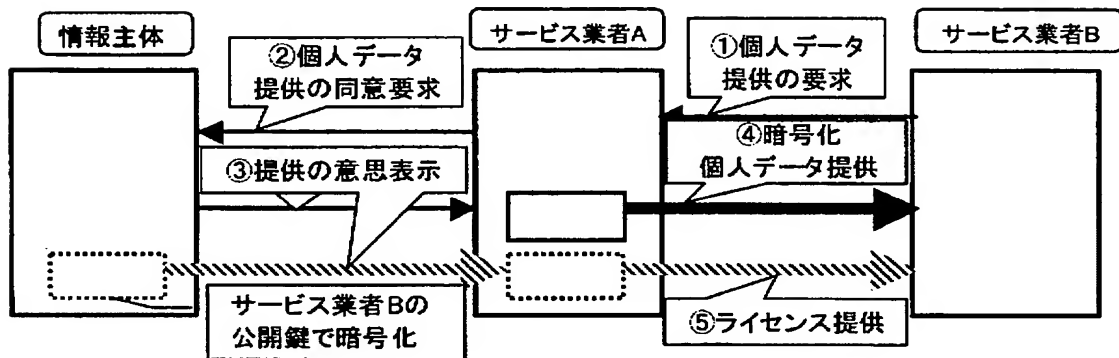


【図 20】

名簿使用時のサービス業者の名簿の
訂正処理を示すフローチャート

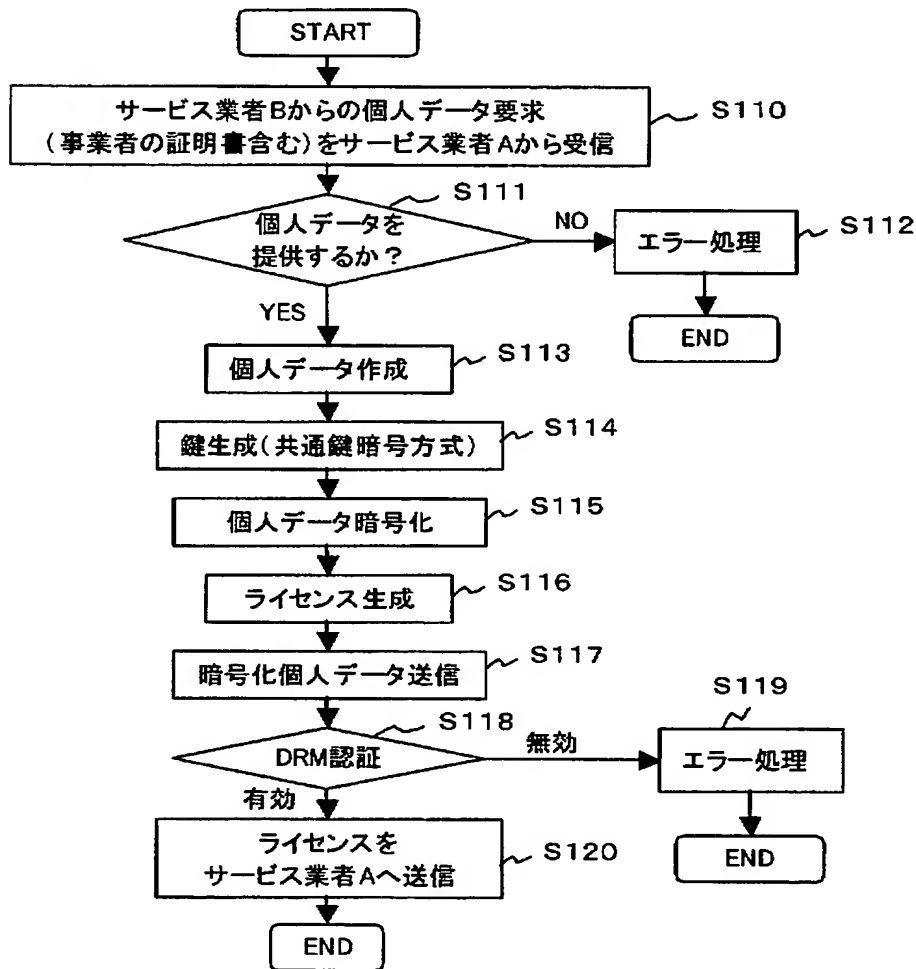
【図 21】

サービス業者間で個人データを取り引きする処理を示す図



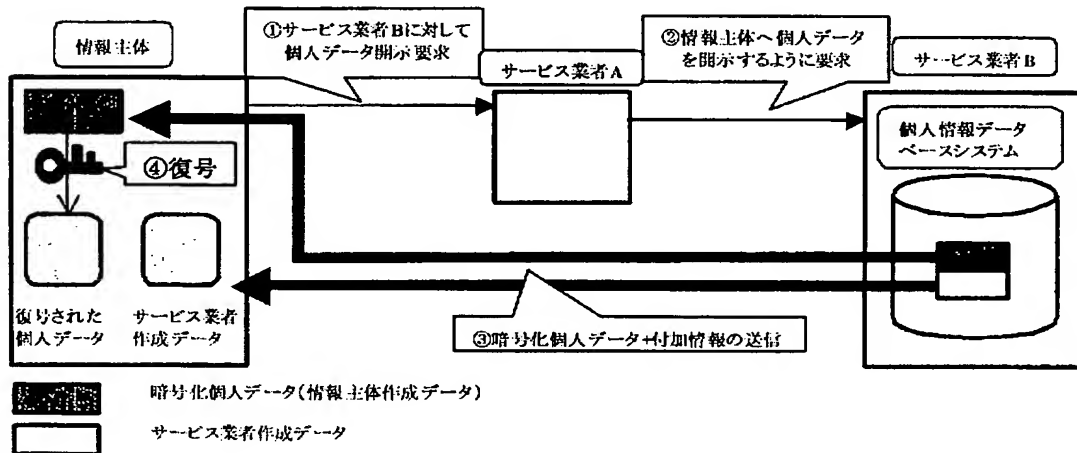
【図 22】

サービス業者Bへの個人データ使用ライセンスを発行するときの
クライアントツールの処理を示すフローチャート



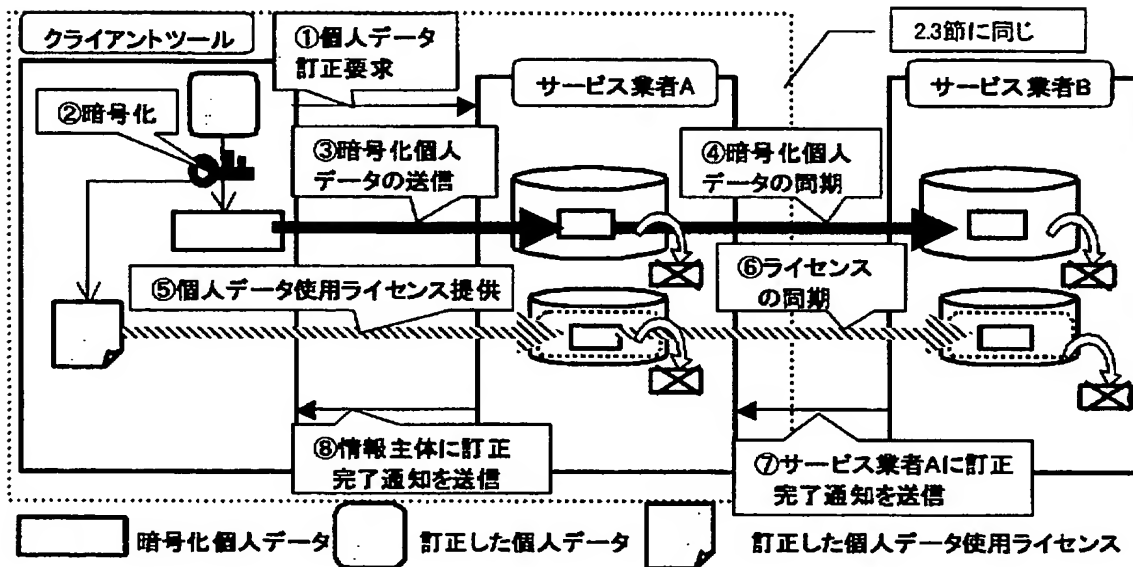
【図 23】

サービス業者間で個人データを取り引きする場合における、
サービス業者Bへの開示請求の処理を説明する図

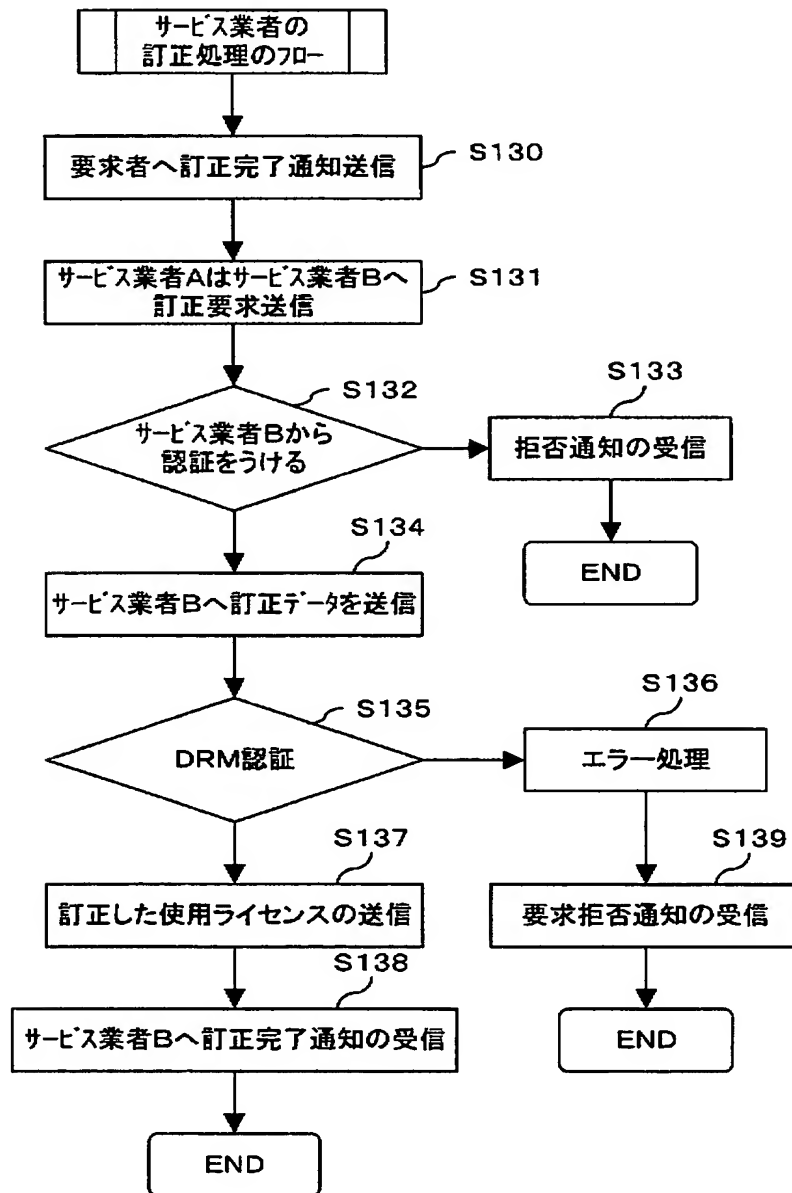


【図 24】

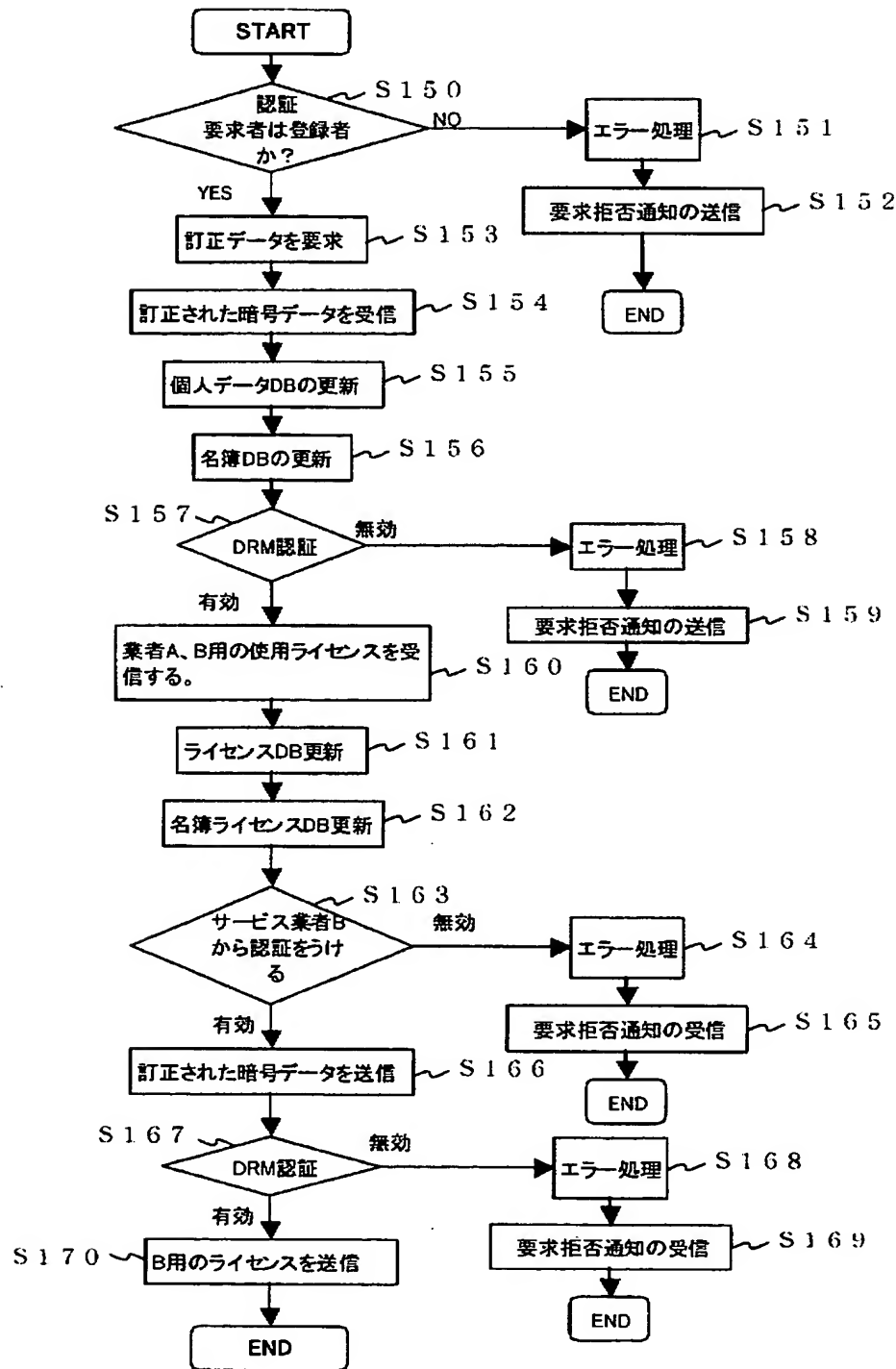
サービス業者間で個人データを取り引きする場合における
訂正請求の処理を説明する図



【図 25】

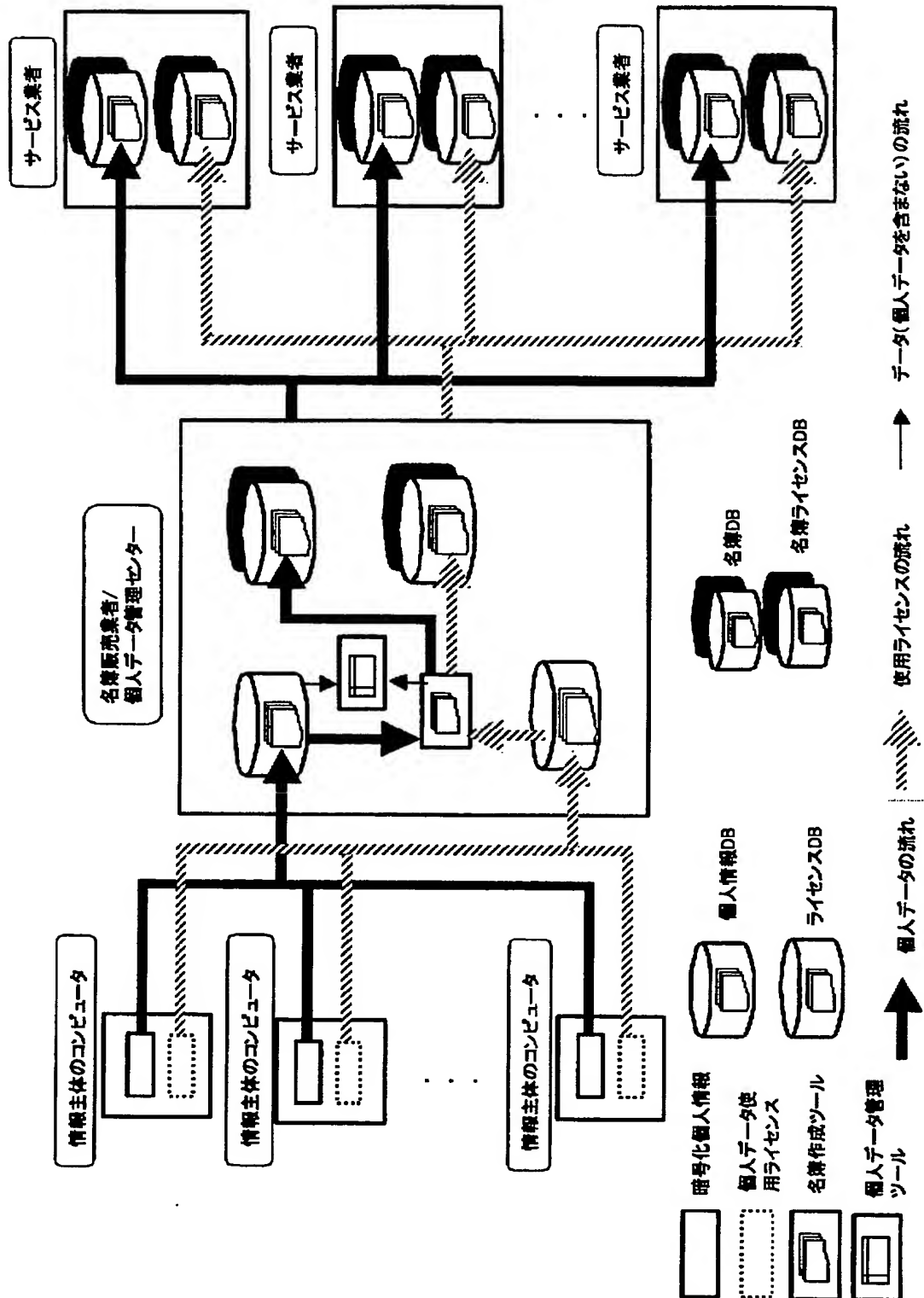
サービス業者間での個人データの同一性を保つための
同期処理を示すフローチャート

【図 27】

名簿を使用する場合の訂正要求における
サービス業者Aの処理のフローチャート

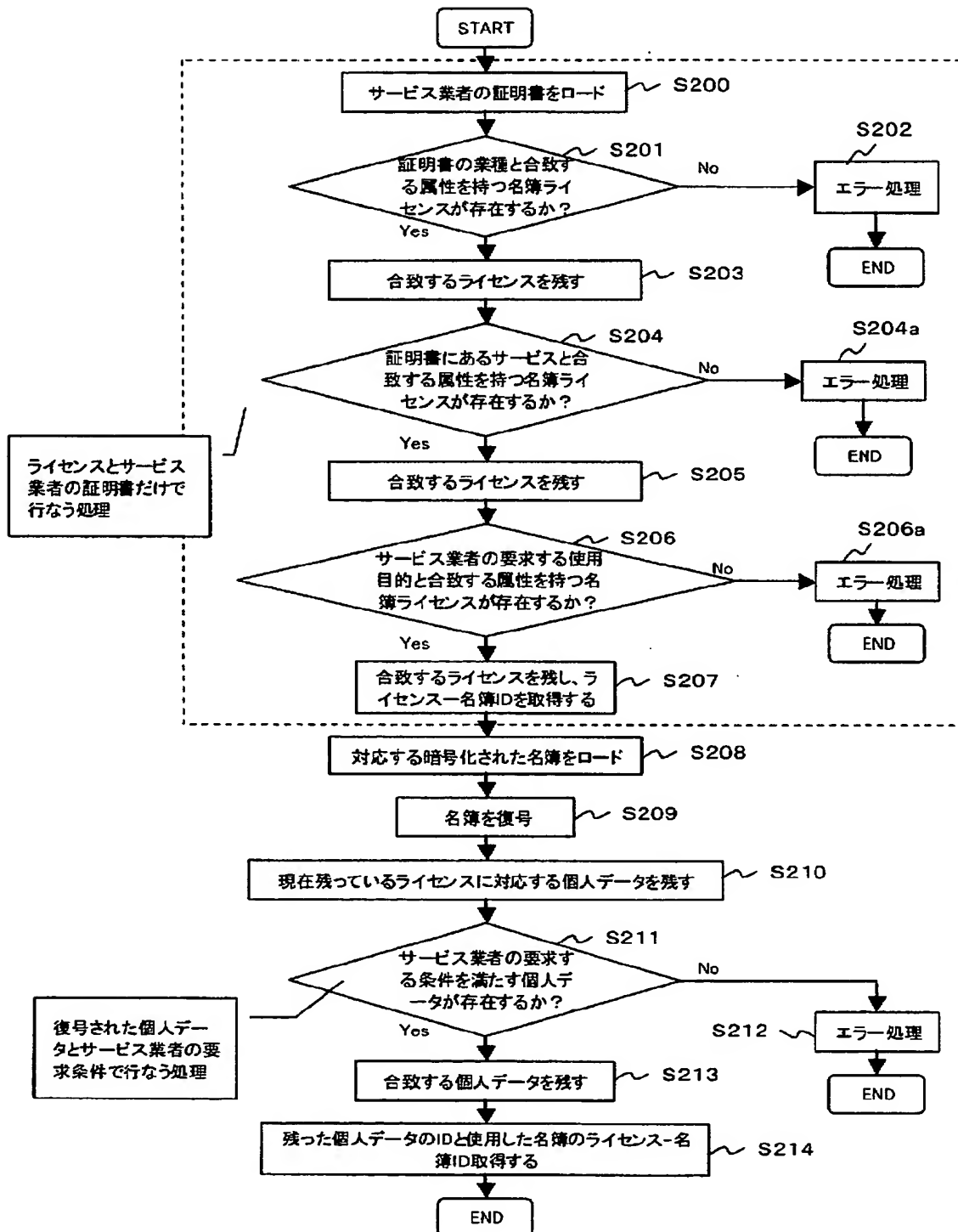
【図 28】

センタ型個人データ提供システムの構成例



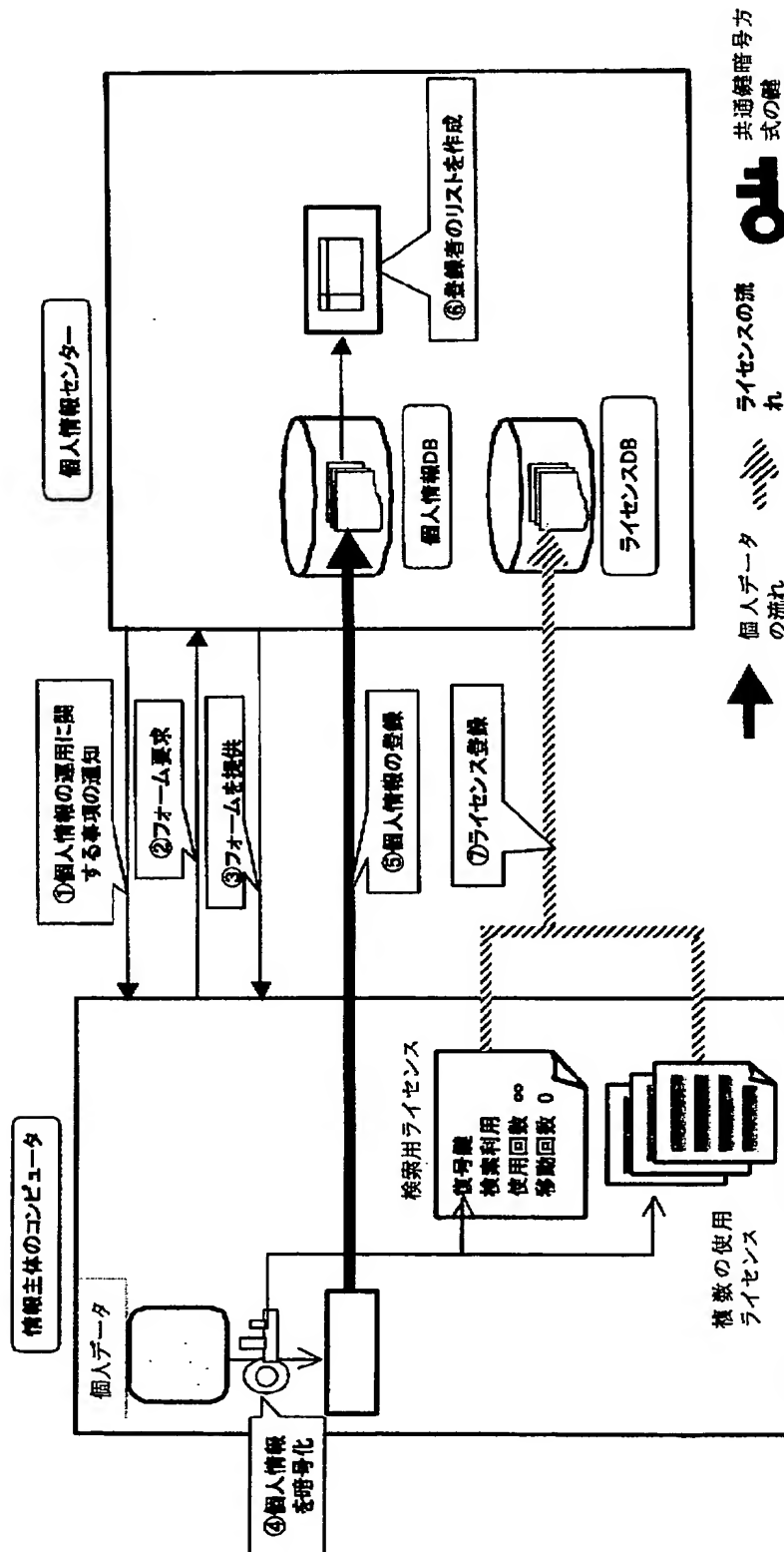
【図 29】

検索ツール処理フローチャートを示す図



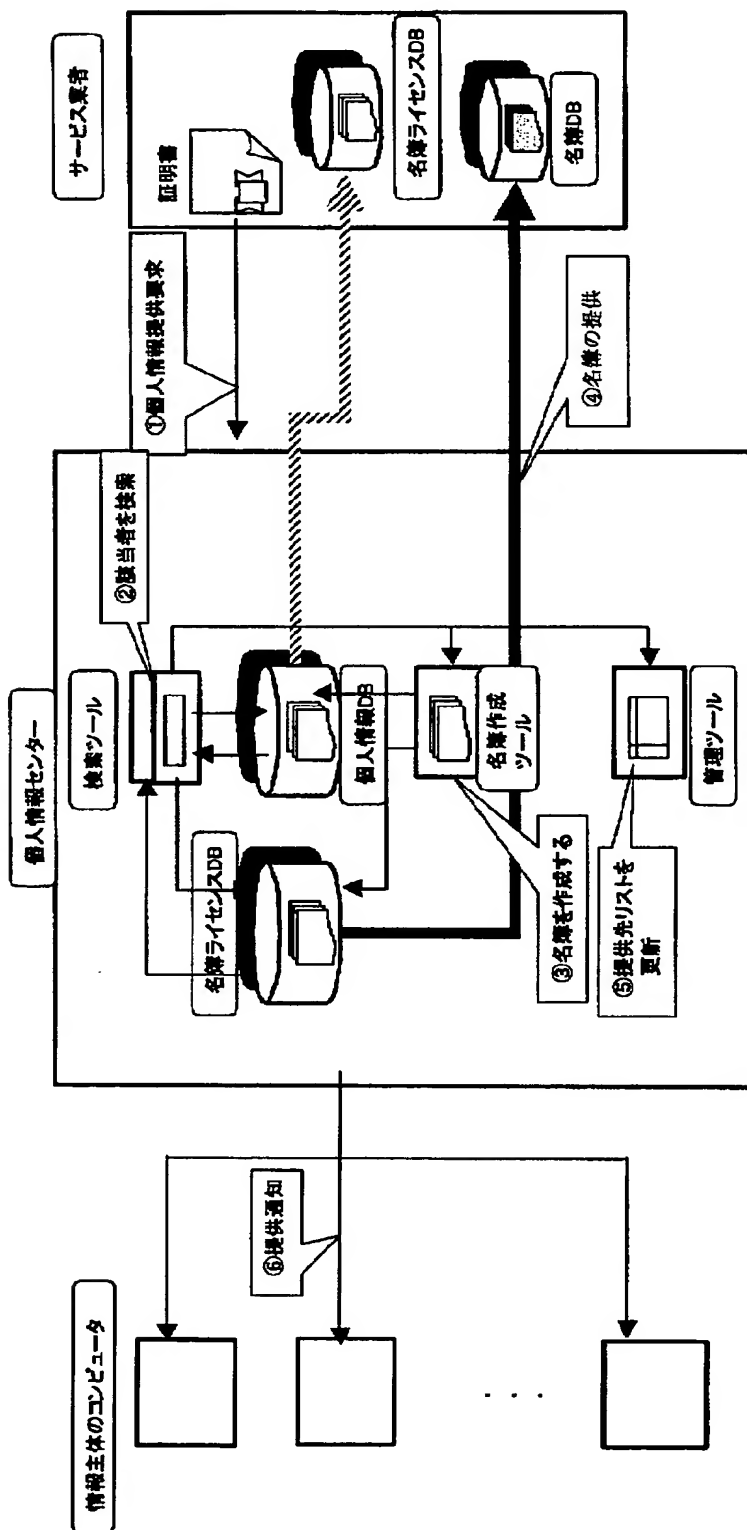
【図 30】

センタへの登録処理を説明する図



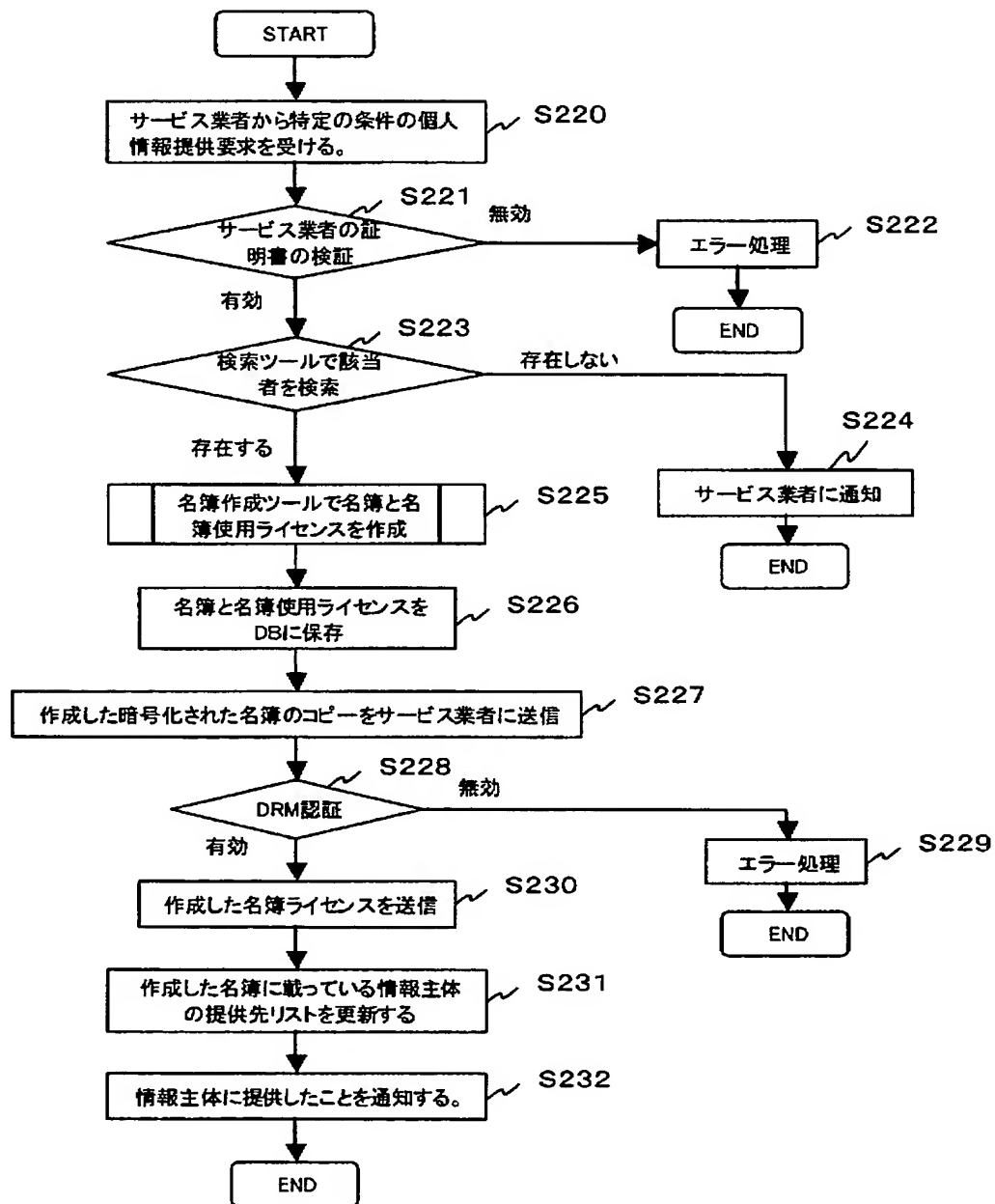
【図 31】

個人データの提供処理を説明する図



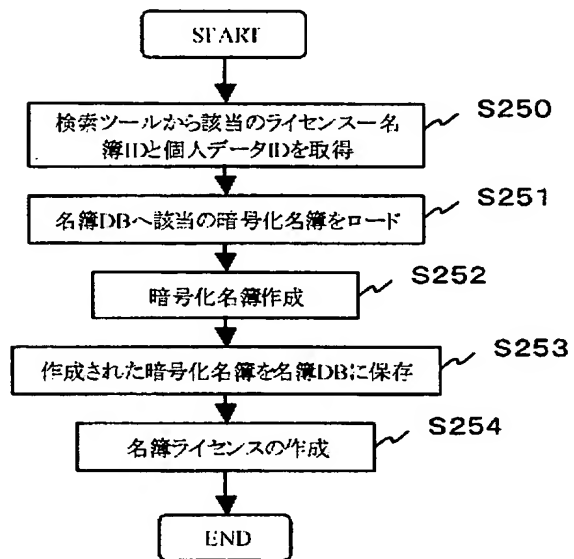
【図 32】

センタの提供処理フローチャート



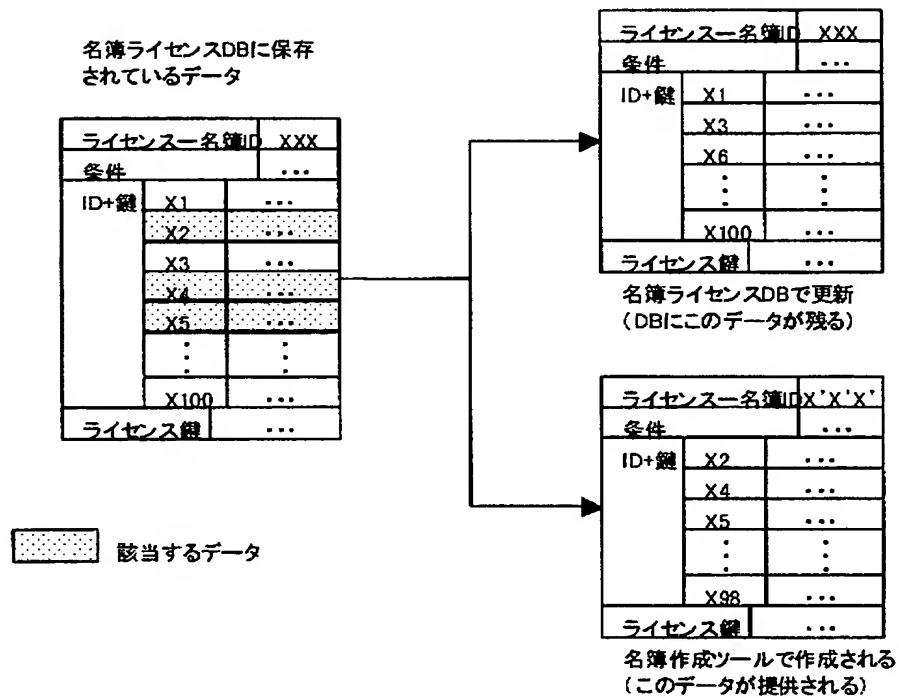
【図 33】

名簿作成ツールのフローチャート



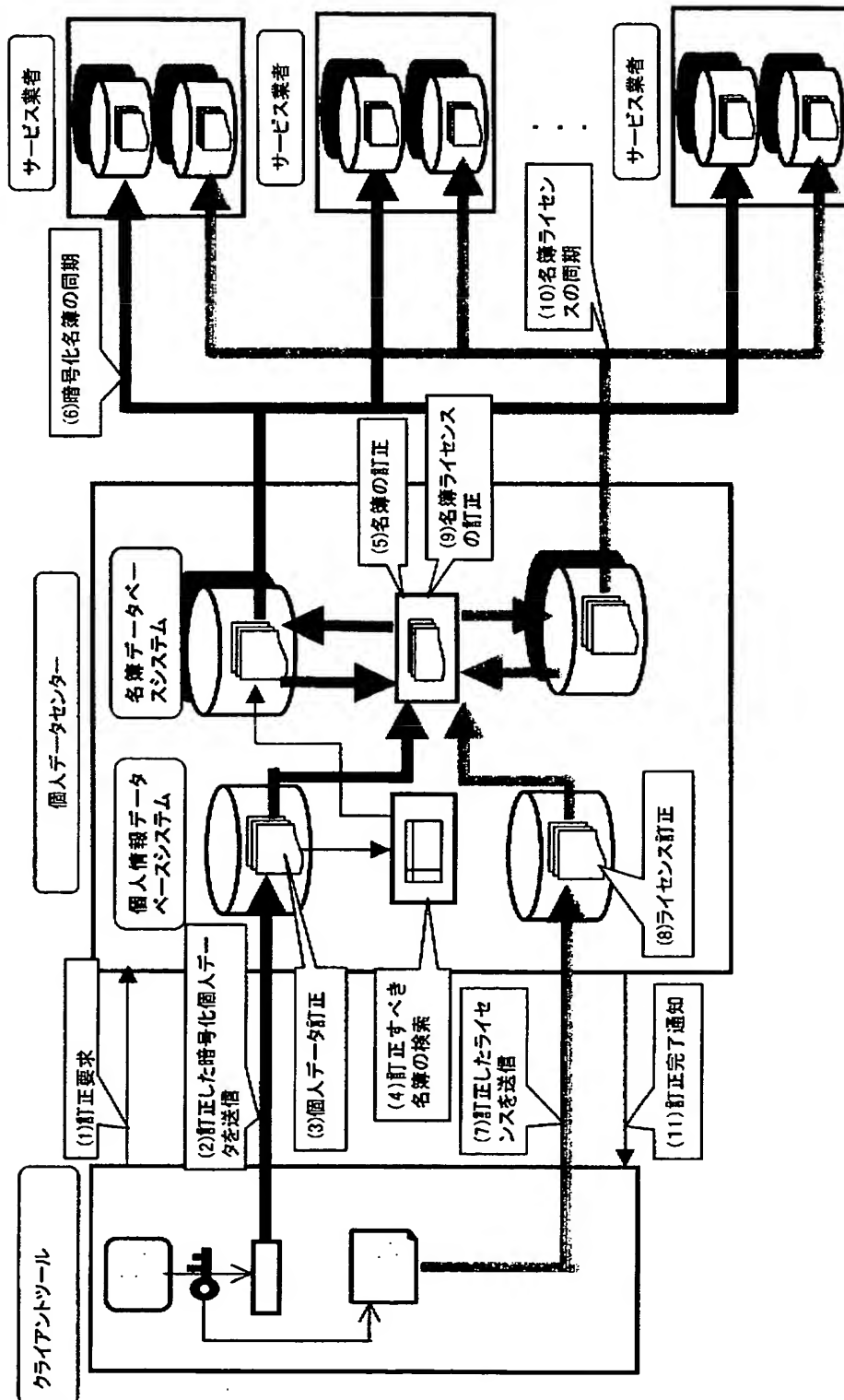
【図 34】

提供される名簿ライセンスの作成の概略を示す図



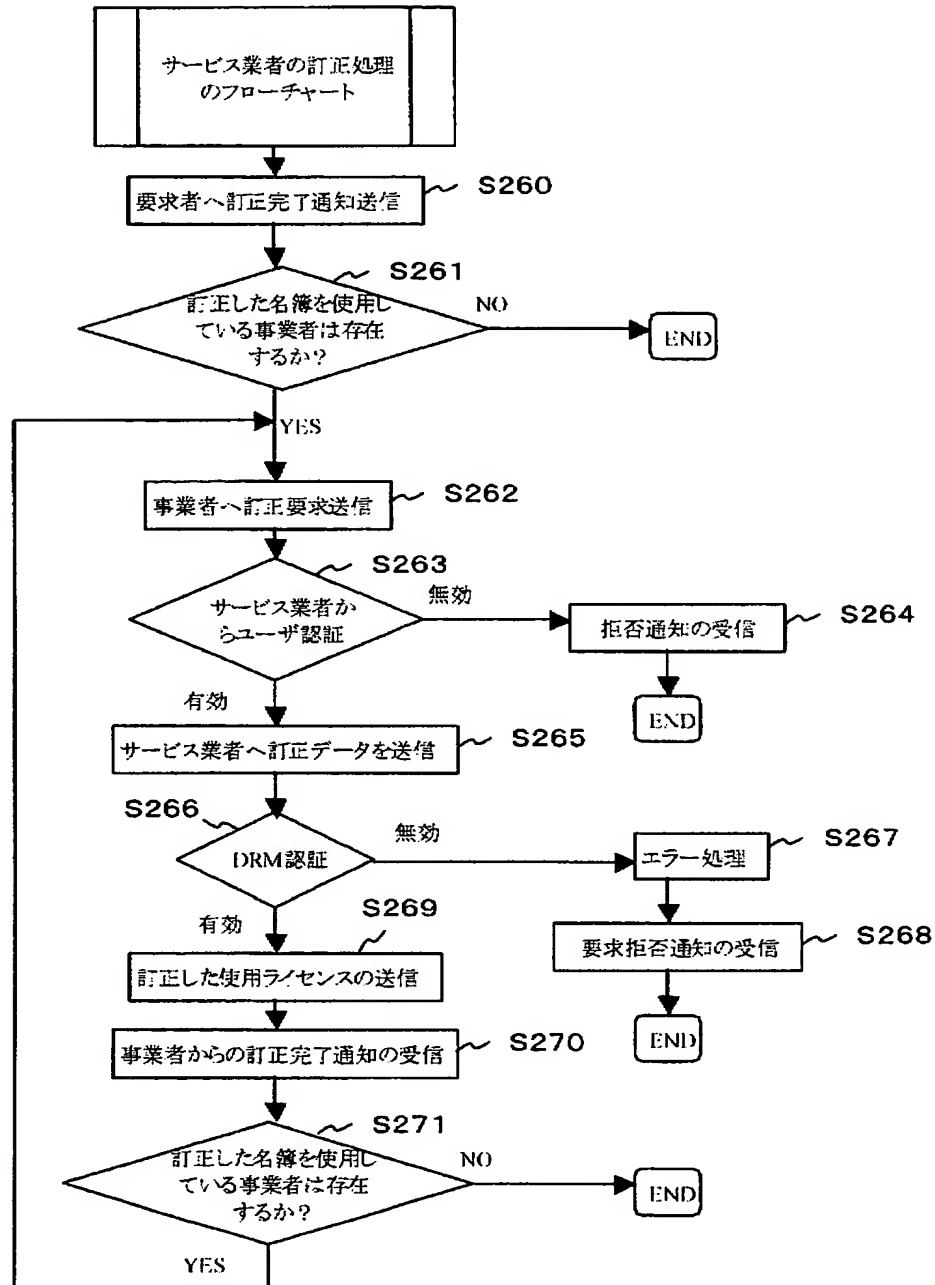
【図 35】

訂正請求の処理の流れを説明した図



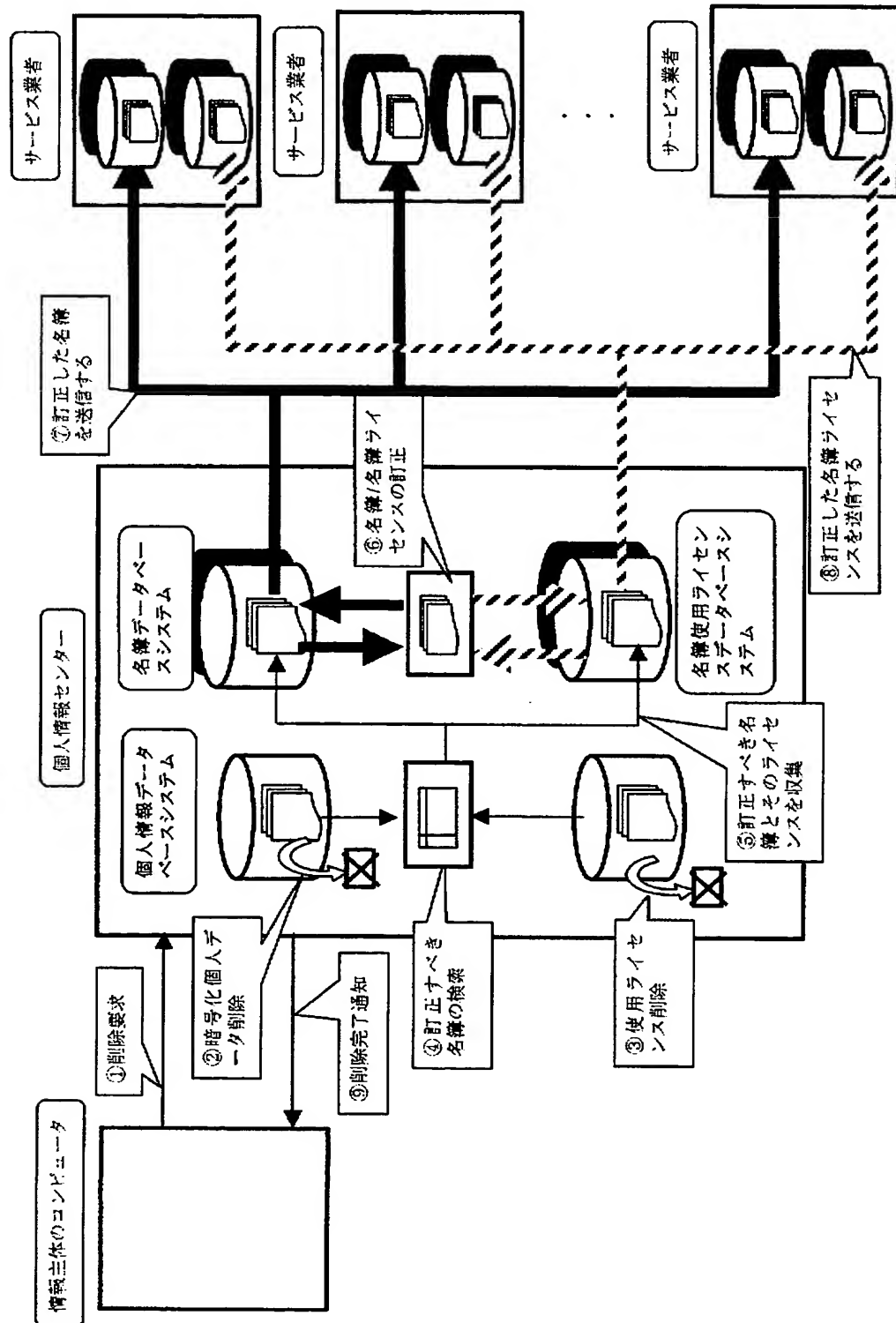
【図 36】

センタの有する個人データの削除処理を説明する図



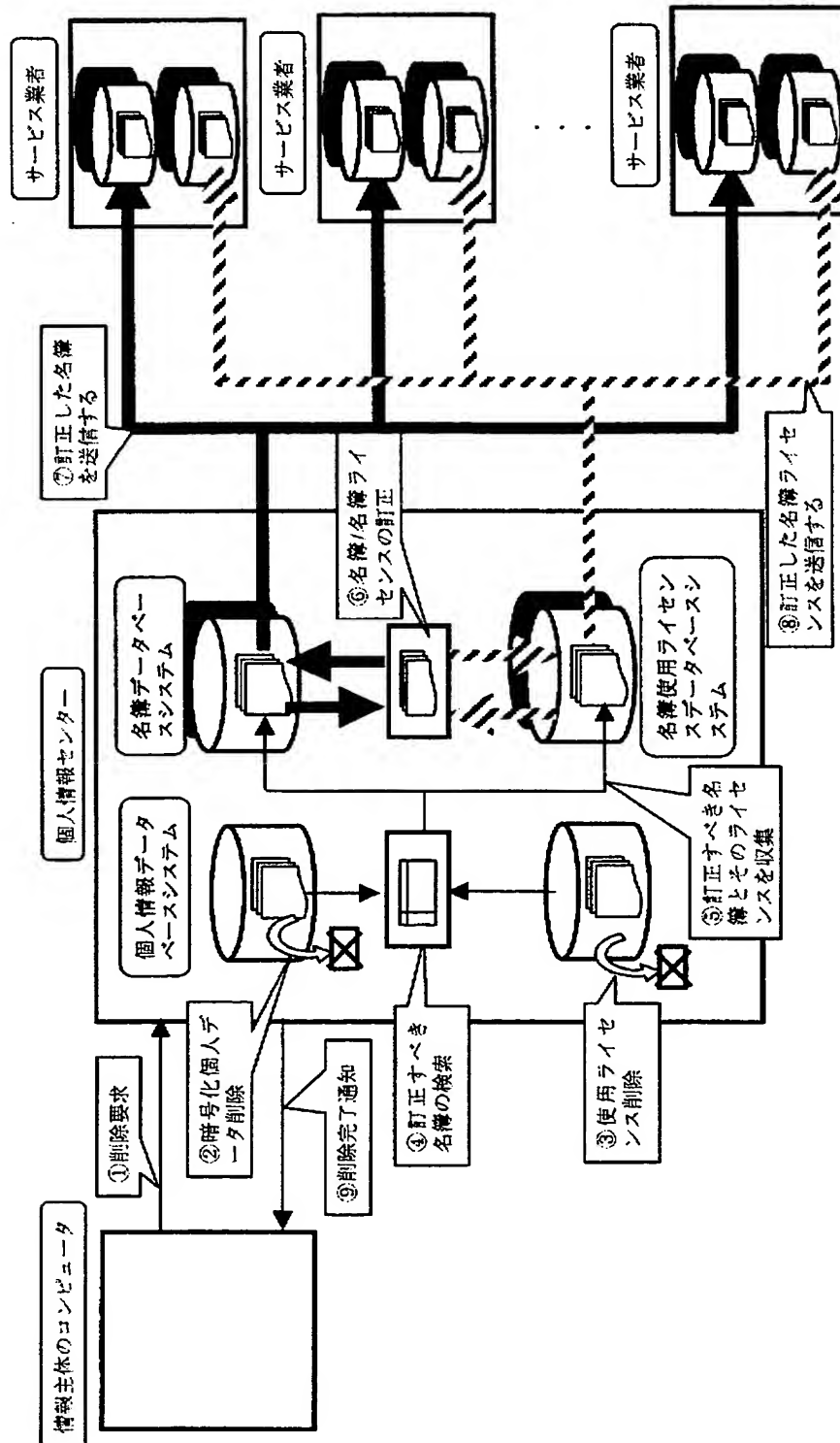
【図 37】

サービス業者が有する個人データの削除処理を説明する図



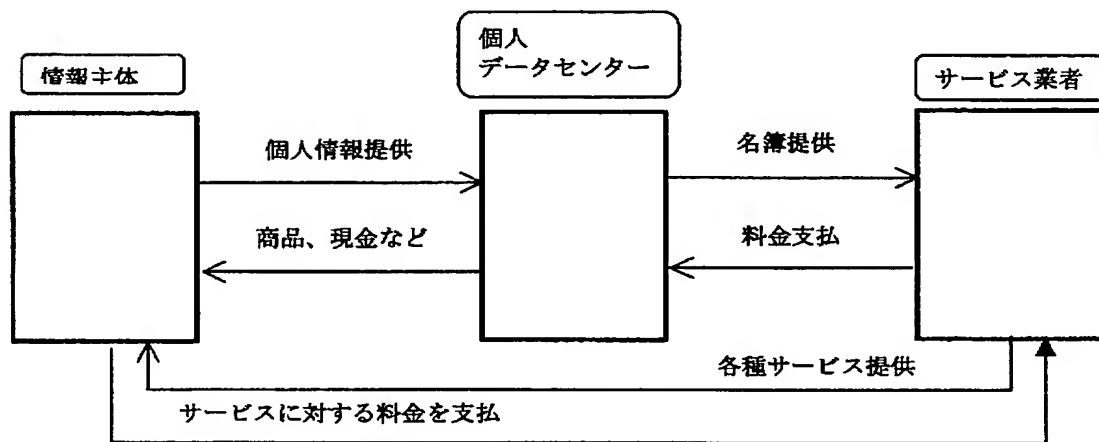
【図 38】

センタの有する個人データの削除処理を説明する図



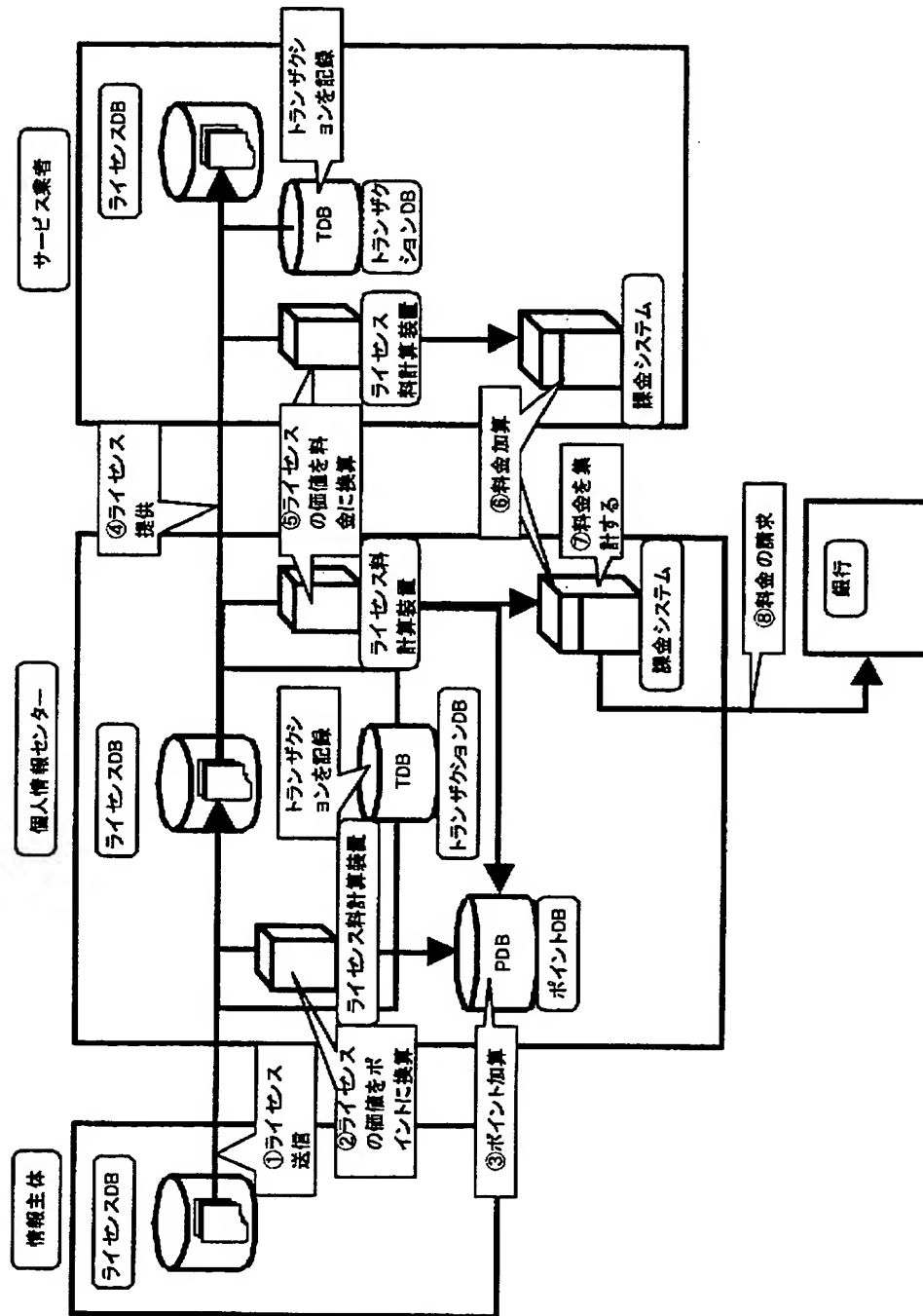
【図 39】

センタ型ビジネスの一形態における情報主体、
センタ、業者の関係を示す図



【図 40】

データの流れを示す図



【書類名】 要約書

【要約】

【課題】 情報主体の制御の下、個人情報の流通を情報主体の意思に従って制御することができる個人情報保護流通システムを提供する。

【解決手段】 情報主体は、クライアントツール 2 0 を使って、個人データの使用を要求するサービス業者のコンピュータ 2 1 に、暗号化された個人データを送る。また、情報主体は、クライアントツール 2 0 を使って、個人データを復号するために使う復号鍵と、利用目的、使用回数、期日、移動可能回数など個人データの利用条件を定めた情報を含めた個人データ使用ライセンスを作成し、D R M 認証技術を使って、サービス業者のコンピュータ 2 1 に送る。サービス業者は、情報主体が作成した個人データ使用ライセンスに記載された使用条件に合致する場合のみ、個人データを使用することができる。

【選択図】 図 3

特願 2 0 0 2 - 2 9 6 7 7 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日
[変更理由]

1 9 9 0 年 8 月 2 4 日
新規登録

住 所
氏 名

神奈川県川崎市中原区上小田中 1 0 1 5 番地
富士通株式会社

2. 変更年月日
[変更理由]

1 9 9 6 年 3 月 2 6 日
住所変更

住 所
氏 名

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
富士通株式会社